ЭЛЕМЕНТЫ МАТЕМАТИКИ

Н. БУРБАКИ

АЛГЕБРА

МНОГОЧЛЕНЫ И ПОЛЯ
УПОРЯДОЧЕННЫЕ ГРУППЫ

ПЕРЕВОД С ФРАНЦУЗСКОГО
В. Е. ГОВОРОВА, Ю. И. МАНИНА,
А. В. МИХАЛЕВА, А. Л. ШМЕЛЬКИНА
ПОД РЕДАКЦИЕЙ Ю. И. МАНИНА

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1965

517
Б 91
УДК 512.8/519.4

АННОТАЦИЯ

Группа французских математиков, объединенных под псевдонимом «Бурбаки», поставила перед собой цель — написать под общим заглавием «Элементы математики» полный трактат по современной математике. Многие выпуски этого трактата уже вышли во Франции, вызвав большой интерес математиков всего мира.

В русском переводе вышли «Топологические векторные пространства» (ИЛ, 1959), «Очерки по истории математики» (ИЛ, 1963), два выпуска «Общей топологии» (Физматгиз, 1958, 1959), один выпуск «Алгебры» (Физматгиз, 1962). Настоящая книга является вторым выпуском «Алгебры», содержащим перевод IV — VI глав.

Книга рассчитана на математиков — научных работников, аспирантов и студентов старших курсов университетов и пединститутов.

Н. Бурбаки

Алгебра (Многочлены и поля. Упорядоченные группы)

М., 1965 г., 300 стр.

Редактор *А. Н. Копылова*

Техн. редактор *Л. Ю. Плакше* Корректор *О. А. Сигал*

Сдано в набор 16/III 1965 г. Подписано к печати 1/VII 1965 г. Бумага 60×90/16. Физ. печ. л. 18,75+3 вкл. Условн. печ. л. 18,75. Уч.-изд. л. 16,65. Тираж 19 500 экз. Цена книги 1 р. 41 к. Заказ № 882.

Издательство «Наука»

Главная редакция физико-математической литературы
Москва, В-71, Ленинский проспект, 15.

Московская типография № 16 Главполиграфпрома Государственного комитета Совета Министров СССР по печати. Москва, Трехпрудный пер., д. 9.

ОГЛАВЛЕНИЕ

Глава IV. Многочлены и рациональные дроби 9
§ 1. Многочлены 9
1. Определение многочленов 9
2. Свойства алгебр многочленов 11
3. Понятие степени 14
4. Многочлены над кольцом целостности 18
5. Евклидово деление многочленов одной переменной 19
§ 2. Полиномиальные функции 26
1. Полиномиальные операторы 26
2. Подстановка многочленов в многочлен 30
3. Полиномиальные функции на алгебре 31
4. Корни многочлена от одной переменной 32
5. Полиномиальные функции на кольце целостности с бесконечным числом элементов 36
§ 3. Рациональные дроби и рациональные функции 42
1. Рациональные дроби над полем 42
2. Рациональные дроби, рассматриваемые как операторы . . . 44
3. Подстановка рациональной дроби в рациональную дробь . . 45
4. Рациональные функции 46
§ 4. Дифференциалы и дифференцирования 48
1. Дифференциалы и производные многочленов 48
2. Приложение: характеризация простых корней многочлена 51
3. Дифференцирования алгебры 52
4. Продолжение дифференцирования; производные рациональных дробей 56
5. Дифференциальные формы 58
6. Приложение к многочленам и рациональным дробям . . . 60
§ 5. Формальные ряды 64
1. Определение формальных рядов 64
2. Порядок формального ряда 66
3. Формальные ряды над областью целостности 68
4. Бесконечные суммы формальных рядов 68
5. Подстановка формальных рядов в формальный ряд 70
6. Обратимые формальные ряды 71

7. Поле дробей кольца формальных рядов от одной переменной над полем 72
8. Дифференцирования в алгебре формальных рядов 73
9. Разрешимость уравнений в кольце формальных рядов . . . 76
10. Топологические интерпретации 77

Глава V. Поля 82

§ 1. Простые поля. Характеристика 82
1. Простые поля 82
2. Характеристическая экспонента 83
3. Характеризация многочленов с нулевой производной . . . 85
§ 2. Расширения 86
1. Структура расширения 87
2. Присоединение 89
3. Линейно разделенные расширения 90
§ 3. Алгебраические расширения 94
1. Алгебраические элементы 94
2. Алгебраические расширения 97
3. Транзитивность алгебраических расширений. Поля, алгебраически замкнутые внутри своего расширения 99
§ 4. Алгебраически замкнутые расширения 101
1. Алгебраически замкнутое поле 101
2. Алгебраически замкнутые расширения 102
§ 5. Трансцендентные расширения 107
1. Алгебраически свободные семейства. Чистые расширения 107
2. Базисы трансцендентности 109
3. Степень трансцендентности расширения 113
4. Алгебраически разделенные расширения 115
§ 6. Продолжения изоморфизмов. Сопряженные элементы. Нормальные расширения 123
1. Продолжения изоморфизмов 123
2. Сопряженные поля. Сопряженные элементы 125
3. Нормальные расширения 127
§ 7. Сепарабельные расширения 132
1. Теорема Артина 132
2. Сепарабельные расширения 135
3. Примеры сепарабельных расширений. Совершенные поля 137
4. Свойства сепарабельных расширений 138
5. Теорема Дедекинда 139
6. Сепарабельные алгебраические элементы 141
7. Примитивные элементы 143
§ 8. Радикальные элементы. Критерий сепарабельности 145
1. Радикальные элементы 145
2. Критерий Маклейна 146
3. Приложение к сепарабельным алгебраическим расширениям 147
4. Радикальные расширения 149

§ 9. Дифференцирования в полях 155
1. Продолжение дифференцирования 156
2. Дифференцирования сепарабельных расширений 160
3. Сепарабельные базисы трансцендентности 161
§ 10. Расширения Галуа 165
1. Определение расширений Галуа 165
2. Подрасширения расширения Галуа 166
3. Семейства расширений Галуа 168
4. Композит расширения Галуа и произвольного расширения 170
5. Теория Галуа 172
6. Норма и след в алгебраических сепарабельных расширениях 174
7. Алгебраическая независимость автоморфизмов 178
8. Нормальный базис расширения Галуа 179
9. Нормальные несепарабельные расширения 181
§ 11. Корни из единицы. Конечные поля. Циклические расширения 185
1. Корни из единицы 185
2. Поле корней n-й степени из единицы 188
3. Конечные поля 191
4. Алгебраические расширения конечной степени конечного поля 192
5. Циклические расширения 193
6. Циклические расширения и двучленные уравнения 196

Приложение I к главе V. Симметрические рациональные дроби . . . 204
1. Симметрические функции 204
2. Симметрические многочлены 206
3. Формула Ньютона 208

Приложение II к главе V. Расширения Галуа бесконечной степени . . 213
1. Топологическая группа Галуа 213
2. Свойства топологических групп Галуа 214

Исторический очерк к главам IV и V 219
Библиография 236

Глава VI. Упорядоченные группы и поля 238
§ 1. Упорядоченные группы. Делимость 238
1. Определение упорядоченных моноидов и групп 238
2. Предупорядоченные и моноиды группы 240
3. Положительные элементы 241
4. Фильтрующиеся группы 242
5. Отношение делимости в поле 243
6. Элементарные операции над упорядоченными группами . . . 246
7. Возрастающие представления упорядоченных групп 247
8. Верхняя и нижняя грани в упорядоченной группе 248
9. Решеточно-упорядоченные группы 250
10. Теорема о разложении 252

11. Положительная и отрицательная части 253
12. Независимые элементы 255
13. Экстремальные элементы 258
§ 2. Упорядоченные поля 271
1. Упорядоченные кольца 271
2. Упорядоченные поля 273
3. Расширение упорядоченных полей 274
4. Алгебраические расширения упорядоченных полей 276
5. Максимальные упорядоченные поля 278
6. Характеризация максимальных упорядоченных полей. Теорема Эйлера — Лагранжа 280
Указатель обозначений 291
Указатель терминов 293
Определения главы IV . . . . . Вклейка 1
Определения главы V . . . . . Вклейка 2
Определения и аксиомы главы VI . . . . . Вклейка 3

ГЛАВА IV

МНОГОЧЛЕНЫ И РАЦИОНАЛЬНЫЕ ДРОБИ

Там, где не оговорено противное, все кольца операторов, рассматриваемые в этой главе, предполагаются коммутативными и имеющими единицу.

§ 1. Многочлены

1. Определение многочленов

Пусть I — произвольное непустое множество индексов, $\boldsymbol{N}^I$ — *произведение* (гл. I, § 4, n° 5) семейства моноидов, имеющее I в качестве множества индексов, причем все моноиды тождественны аддитивному моноиду $\boldsymbol{N}$ целых положительных чисел. Пусть $\boldsymbol{N}^{(I)}$ — устойчивое подмножество в $\boldsymbol{N}^I$, состоящее из последовательностей (n_ι), у которых $n_\iota = 0$ для всех индексов ι, кроме конечного числа. Если I конечно, то $\boldsymbol{N}^{(I)}$ и $\boldsymbol{N}^I$ совпадают. Пусть A — некоторое коммутативное кольцо с единицей. Рассмотрим *алгебру моноида* $\boldsymbol{N}^{(I)}$ относительно кольца A (гл. II, § 7, n° 9). Эта алгебра обладает каноническим базисом $(e_{(n_\iota)})_{(n_\iota)\in \boldsymbol{N}^{(I)}}$ со следующей таблицей умножения: $e_{(m_\iota)} \cdot e_{(n_\iota)} = e_{(m_\iota + n_\iota)}$. Она *коммутативна*. Роль *единицы* играет элемент e_ω канонического базиса, где ω есть элемент из $\boldsymbol{N}^{(I)}$, все координаты которого равны нулю. Поскольку элемент e_ω является свободным, можно отождествить кольцо A с подалгеброй Ae_ω, установив соответствие $\lambda \longrightarrow \lambda e_\omega$, которое отождествляет e_ω с единицей кольца A (мы будем обозначать ее через 1, если это не приведет к путанице).

Для каждого индекса $\varkappa \in I$ рассмотрим элемент $(n_\iota) \in \boldsymbol{N}^{(I)}$ такой, что $n_\varkappa = 1$ и $n_\iota = 0$ при $\iota \neq \varkappa$. Элемент $e_{(n_\iota)}$ канонического

базиса, соответствующий элементу $(n_\iota) \in \boldsymbol{N}^{(I)}$, обозначим символом $X_\varkappa$. Из приведенной выше таблицы умножения (с помощью индукции по n_ι) легко усмотреть, что каждый элемент $e_{(n_\iota)}$ канонического базиса можно записать единственным образом в виде $e_{(n_\iota)} = \prod_{\iota \in I} X_\iota^{n_\iota}$ (выражение имеет смысл, поскольку все n_ι, за исключением конечного числа из них, равны нулю).

Таким образом, алгебра моноида $\boldsymbol{N}^{(I)}$ *порождается* элементами 1 и X_ι (где ι пробегает I).

Определение 1. *Алгебра моноида* $\boldsymbol{N}^{(I)}$ *относительно кольца* A (коммутативного и обладающего единицей) *называется алгеброй многочленов относительно переменных* X_ι $(\iota \in I)$ *с коэффициентами из кольца* A *и обозначается символом* $A[X_\iota]_{\iota \in I}$. *Элементы этой алгебры называются многочленами относительно переменных* X_ι $(\iota \in I)$ *с коэффициентами из кольца* A.

Пусть I — конечное подмножество в $\boldsymbol{N}$. Вместо $A[X_\iota]_{\iota \in I}$ мы пишем $A[X_{i_1}, X_{i_2}, \ldots, X_{i_p}]$, где $(i_k)_{1 \leqslant k \leqslant p}$ — последовательность элементов из I, расположенная в порядке возрастания.

Каждый многочлен $u \in A[X_\iota]_{\iota \in I}$ записывается единственным образом в виде $u = \sum_{(n_\iota)} a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$, где индекс (n_ι) пробегает множество $\boldsymbol{N}^{(I)}$. Элементы $a_{(n_\iota)}$, из которых только конечное число отлично от нуля, называются *коэффициентами* многочлена u, а элементы $a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ называются его *членами* (элемент $a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ будет часто называться «членом при $\prod_{\iota \in I} X_\iota^{n_\iota}$»; когда все n_ι равны нулю, его называют также «свободным членом» многочлена (ср. § 2)). Элементы $\prod_{\iota \in I} X_\iota^{n_\iota}$ канонического базиса алгебры $A[X_\iota]_{\iota \in I}$ называются *одночленами*: каждый многочлен, таким образом, является линейной комбинацией одночленов с коэффициентами из A, причем одночлены линейно независимы.

Если коэффициент $a_{(n_\iota)}$ многочлена u равен нулю, то говорят (для краткости), что u *не содержит члена при* $\prod_{\iota \in I} X_\iota^{n_\iota}$. В частности, если «свободный член» многочлена u равен нулю, то говорят, что u — многочлен «без свободного члена».

2. Свойства алгебр многочленов

Пусть I и I' — два множества одинаковой мощности, и пусть φ — взаимно однозначное отображение I на I'. Линейное отображение алгебры $A[X_\iota]_{\iota\in I}$ на алгебру $A[X_\varkappa]_{\varkappa\in I'}$, которое каждому элементу $\prod_{\iota\in I} X_\iota^{n_\iota}$ канонического базиса алгебры $A[X_\iota]_{\iota\in I}$ ставит в соответствие элемент $\prod_{\iota\in I} X_{\varphi(\iota)}^{n_\iota}$ канонического базиса алгебры $A[X_\varkappa]_{\varkappa\in I'}$, есть *изоморфизм* первой из этих алгебр многочленов на вторую.

В частности, алгебры многочленов с коэффициентами из кольца A, соответствующие всевозможным *конечным* множествам индексов с одним и тем же числом элементов n, изоморфны между собой. Их отождествляют обычно с алгеброй многочленов, соответствующей множеству индексов $I=[1, n]$ и называют *алгебрами многочленов от n переменных* с коэффициентами из кольца A.

Естественно, для обозначения переменных можно пользоваться любыми другими буквами вместо букв X_i $(1\leqslant i\leqslant n)$. Например, в многочленах от трех переменных переменные можно обозначать символами Y_1, Y_2, Y_3 или X, Y, Z. Каковы бы ни были принятые обозначения, будем иметь в виду, что речь идет всегда об одной и той же алгебре, структура A-модуля которой совпадает со структурой модуля $A^{(N3)}$, и что три переменные—это три элемента e_{100}, e_{010}, e_{001} канонического базиса этого модуля.

В частности, когда мы будем говорить о многочленах от одной переменной, эта переменная будет чаще всего обозначаться через X, а алгебра многочленов от одной переменной—символом $A[X]$. Таким образом, каждый многочлен $u\in A[X]$ записывается единственным образом в виде $\sum_{n\in N} a_n X^n$. Сумма и произведение двух многочленов от X, $u=\sum_n a_n X^n$, $v=\sum_n \beta_n X^n$, задаются формулами

$$u+v=\sum_n (a_n+\beta_n)\, X^n, \tag{1}$$

$$uv=\sum_n vX^n, \quad \text{где} \quad v=\sum_{p=0}^{n} a_p\beta_{n-p}. \tag{2}$$

Пусть J — произвольное непустое подмножество множества I. Моноид $N^{(J)}$ можно отождествить с устойчивым подмножеством в $N^{(I)}$, состоящим из элементов (n_ι), у которых $n_\iota=0$

при всех $\iota \in CJ$. Следовательно (гл. II, § 7, n° 9), алгебру $A[X_\iota]_{\iota\in J}$ можно отождествить с *подалгеброй* $A[X_\iota]_{\iota\in I}$, имеющей в качестве базиса одночлены $\prod_{\iota\in I} X_\iota^{n_\iota}$, где $n_\iota = 0$ для всех $\iota \in CJ$. Эта подалгебра порождена элементами 1 и X_ι, $\iota \in J$. Иногда говорят, что она состоит из многочленов, *не содержащих* X_ι, где $\iota \in CJ$.

При $J = \varnothing$ подалгебра алгебры $A[X_\iota]_{\iota\in I}$, порожденная элементами 1 и X_ι, $\iota \in J$, сводится к A. Мы условимся применять обозначение $A[X_\iota]_{\iota\in\varnothing}$ и в этом случае.

Осуществленное отождествление позволяет говорить о том, что алгебра $A[X_\iota]_{\iota\in I}$ является *объединением* подалгебр $A[X_\iota]_{\iota\in J}$, где J пробегает множество всех *конечных* подмножеств множества I. Действительно, каждый многочлен u является суммой конечного числа ненулевых членов вида $a_{(n_\iota)}\prod_\iota X_\iota^{n_\iota}$. В каждом из этих членов число индексов ι, для которых $n_\iota \neq 0$, конечно. Обозначим буквой J конечную часть I, состоящую из всех таких индексов (соответствующих всем ненулевым членам многочлена u). Тогда, очевидно, u принадлежит алгебре $A[X_\iota]_{\iota\in J}$.

Для любых двух равномощных подмножеств J и J' множества I подалгебры $A[X_\iota]_{\iota\in J}$ и $A[X_\iota]_{\iota\in J'}$ алгебры $A[X_\iota]_{\iota\in I}$ изоморфны. Например, в алгебре $A[X, Y, Z]$ многочленов от трех переменных над кольцом A алгебры $A[X]$, $A[Y]$, $A[Z]$ изоморфны, но, разумеется, не тождественны. Заметим по этому поводу, что пока в некотором рассуждении участвуют только многочлены от одной переменной, нет смысла различать алгебры $A[X]$, $A[Y]$, $A[Z]$ и т. д., как мы об этом говорили выше. Напротив, во всех рассуждениях, где участвуют многочлены от нескольких переменных X, Y, Z и т. д., эти обозначения применяются к различным алгебрам.

Пусть J — непустое подмножество множества I, отличное от I, $K = CJ$ — дополнение J в I. Моноид $\boldsymbol{N}^{(I)}$ изоморфен произведению моноидов $\boldsymbol{N}^{(J)} \times \boldsymbol{N}^{(K)}$ (гл. I, § 4, n° 5). Отсюда следует (гл. III, § 3, n° 2), что алгебра $A[X_\iota]_{\iota\in I}$ изоморфна тензорному произведению подалгебр $A[X_\iota]_{\iota\in J}$ и $A[X_\iota]_{\iota\in K}$.

Этот результат можно получить другим способом, заметив, что алгебра $A[X_\iota]_{\iota\in I}$ изоморфна тензорному произведению алгебр $A[X_\iota]$ многочленов от одной переменной, что тотчас следует из вида канонического базиса алгебры $A[X_\iota]_{\iota\in I}$ (гл. III, Приложение 1).

Пусть $B = A[X_\iota]_{\iota\in J}$. Кольцо $A[X_\iota]_{\iota\in I}$, рассматриваемое как алгебра относительно своего подкольца B, есть не что иное, как алгебра, полученная путем *расширения* кольца операторов A алгебры $A[X_\iota]_{\iota\in K}$ до кольца B (гл. III, § 3, n° 4). Другими словами, каждый многочлен относительно переменных X_ι, $\iota\in I$, с коэффициентами из кольца A можно однозначно подставить в виде многочлена относительно переменных X_ι, $\iota\in J$, с коэффициентами из кольца B многочленов относительно X_ι, $\iota\in J$ (с коэффициентами из кольца A). Алгебра $A[X_\iota]_{\iota\in I}$, как алгебра над кольцом B, отождествляется, таким образом, с алгеброй многочленов $B[X_\iota]_{\iota\in K}$.

Предложение 1. *Пусть φ — представление кольца A в кольцо B, переводящее единичный элемент кольца A в единичный элемент кольца B. При этих условиях существует единственное представление $\overline{\varphi}$ кольца $A[X_\iota]_{\iota\in I}$ в кольцо $B[X_\iota]_{\iota\in I}$, которое продолжает φ и для любого $\iota\in I$ отображает многочлен X_ι кольца $A[X_\iota]_{\iota\in I}$ в многочлен X_ι кольца $B[X_\iota]_{\iota\in I}$. При этом, если φ — изоморфизм кольца A на кольцо B, то $\overline{\varphi}$ — изоморфизм $A[X_\iota]_{\iota\in I}$ на $B[X_\iota]_{\iota\in I}$.*

Это частный случай общего предложения о моноидных алгебрах (гл. II, § 7, n° 9). Точнее говоря, образом относительно отображения $\overline{\varphi}$ многочлена $\sum_{(n_\iota)} a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$ является многочлен $\sum_{(n_\iota)} \varphi(a_{(n_\iota)}) \prod_\iota X_\iota^{n_\iota}$. Говорят, что последний многочлен получен *применением φ к коэффициентам многочлена* $\sum_{(n_\iota)} a_{(n_\iota)} \prod X_\iota^{n_\iota}$.

В формулировке предложения 1 нам надо было подчеркнуть разницу между многочленом X_ι кольца $A[X_\iota]_{\iota\in I}$ и многочленом X_ι кольца $B[X_\iota]_{\iota\in I}$ (эти многочлены различаются в силу их определения (n°1)). Однако, допуская вольность речи, их обычно отождествляют и говорят, что представление $\overline{\varphi}$ оставляет *инвариантным* каждый многочлен X_ι.

В частности, если A' есть подкольцо кольца A, имеющее тот же самый единичный элемент, то каноническое вложение A' в A продолжается до канонического вложения подкольца $A'[X_\iota]_{\iota\in I}$ в кольцо $A[X_\iota]_{\iota\in I}$. Сужая кольцо операторов алгебры $A[X_\iota]_{\iota\in I}$

до A', мы можем рассматривать алгебру $A[X_\iota]_{\iota\in I}$ как алгебру над A'. Алгебра $A'[X_\iota]_{\iota\in I}$ является в этом случае подалгеброй алгебры $A[X_\iota]_{\iota\in I}$ (см. гл. II, § 7, n° 9).

3. Понятие степени

Определение 2. *Членами полной степени p в многочлене $u\in A[X_\iota]_{\iota\in I}$ называются члены $a_{(n_\iota)}\prod_\iota X_\iota^{n_\iota}$, у которых $\sum_{\iota\in I} n_\iota = p$.*

Сумма всех членов полной степени p многочлена u называется однородной составляющей (полной) степени p многочлена u. Говорят, что u является однородным многочленом полной степени p, если он равен своей однородной составляющей полной степени p.

Предложение 2. *Если u и v — два однородных многочлена степеней p и q соответственно, то uv есть однородный многочлен степени $p+q$.* Предложение вытекает, очевидно, из определения 2.

Ясно, что множество однородных многочленов полной степени p является *подмодулем* H_p в кольце $A[X_\iota]_{\iota\in I}$ (рассматриваемом как A-модуль) с базой, состоящей из одночленов $\prod_\iota X_\iota^{n_\iota}$, у которых $\sum_\iota n_\iota = p$ (p — произвольное неотрицательное целое число). Отсюда следует, что A-модуль $A[X_\iota]_{\iota\in I}$ есть *прямая сумма* подмодулей H_p ($p\in \mathbf{N}$). Поэтому произвольный многочлен u однозначно представляется в виде $u=\sum_{p=0}^{\infty} u_p$, $u_p\in H_p$, где u_p — однородная составляющая степени p многочлена u ($u_p=0$ для всех индексов p, за исключением конечного числа).

Пусть I — *конечное* множество из q элементов, например $I=[1, q]$. Число одночленов полной степени p равно числу элементов $(n_k)_{1\leqslant k\leqslant q}$ из $\mathbf{N}^q$, у которых $\sum_{k=1}^{q} n_k = p$, т. е. $\binom{q+p-1}{p}$ (Теор. мн., гл. III). Таким образом, подмодуль H_p допускает базис из $\binom{q+p-1}{p}$ элементов (см. гл. III, § 5, следствие 2 к теореме 2).

Пересечение двух различных модулей H_p равно нулю. Следовательно, каждый ненулевой однородный многочлен u может

принадлежать только одному из H_p. Число p, для которого $u \in H_p$, называется (полной) *степенью* многочлена u. Более общо введем следующее определение:

Определение 3. *Назовем (полной) степенью ненулевого многочлена u и обозначим символом* $\deg u$ *наибольшее из целых чисел $p \geqslant 0$, для которых однородная составляющая степени p многочлена u отлична от нуля.*

Замечания. 1) Стоит отметить, что, согласно определениям 2 и 3, *степень нулевого многочлена не определена*, но что для *всякого* целого числа $p \geqslant 0$ мы тем не менее имеем право сказать, что «нуль является однородным многочленом степени p». В этом заключается традиционная вольность речи, так как вторую фразу надо понимать как синоним «$0 \in H_p$». Иначе говоря, в этой фразе слово «степень» не следует отделять от выражения «однородный многочлен степени p», которое должно рассматриваться как единый термин.

Точно так же удобно говорить, что «f есть многочлен степени $\leqslant p$ (соответственно $< p$)», если однородная часть степени n многочлена f равна нулю при всех $n > p$ (соответственно $n \geqslant p$). Это выражение означает, таким образом, что многочлен f *равен нулю или степень его* $\leqslant p$ (соответственно $< p$) и выражение «многочлен степени $\leqslant p$» (соответственно «многочлен степени $< p$») должно также рассматриваться как единый термин.

2) Однородные многочлены степени p называют также (допуская вольность речи; см § 2) *формами степени p* относительно переменных X_ι. В частности, каждая форма степени 1 (соответственно 2, 3, 4) называется *линейной формой* (соответственно *квадратичной*, *кубичной*, *биквадратичной*). Формы относительно n переменных называются *n-арными формами* (*бинарными*, *тернарными*, *кватернарными*—для $n=2$, 3, 4 соответственно).

3) Однородные многочлены нулевой степени являются не чем иным, как элементами кольца A. Говорнт еще, что они являются *константами* в кольце $A[X_\iota]_{\iota \in I}$ (см. § 2).

Предложение 3. *Пусть u и v — два многочлена, не равные нулю одновременно.*

1° *Если* $\deg u \neq \deg v$, *то*

$$u + v \neq 0 \quad \text{и} \quad \deg(u+v) = \operatorname{Max}(\deg u,\ \deg v).$$

Если $\deg u = \deg v$ *и, кроме того,* $u + v \neq 0$, *то*

$$\deg(u+v) \leqslant \operatorname{Max}(\deg u,\ \deg v). \tag{3}$$

2° *Если* $uv \neq 0$, *то*

$$\deg(uv) \leqslant \deg u + \deg v. \tag{4}$$

Доказательства очевидны.

Из формул (3) и (4) (вторая применима в случае, когда $\deg u = 0$) вытекает, что многочлены полной степени $\leqslant p$ образуют *подмодуль* в $A[X_\iota]_{\iota\in I}$, база которого состоит из одночленов $\prod_\iota X_\iota^{n_\iota}$, у которых $\sum_\iota n_\iota \leqslant p$.

Пусть теперь J — некоторое непустое подмножество множества I. Мы видели, что каждый многочлен u из кольца $A[X_\iota]_{\iota\in I}$ можно рассматривать как многочлен относительно переменных X_ι, $\iota\in J$, с коэффициентами из кольца многочленов $B = A[X_\iota]_{\iota\in CJ}$. Определения 2 и 3 применимы, естественно, к кольцу $B[X_\iota]_{\iota\in J}$. Им соответствуют новые определения для многочленов $u\in A[X_\iota]_{\iota\in I}$: мы будем говорить, что член $a_{(n_\iota)}\prod_\iota X_\iota^{n_\iota}$ имеет *степень* p *относительно* переменных X_ι, $\iota\in J$, если $\sum_{\iota\in J} n_\iota = p$. Многочлен u называется *однородным*, *причем степени* p, *относительно* переменных X_ι, $\iota\in J$, если все ненулевые члены многочлена имеют относительно этих неизвестных степень p. Множество таких многочленов образует подмодуль в кольце $A[X_\iota]_{\iota\in I}$, а $A[X_\iota]_{\iota\in I}$ является *прямой суммой* подмодулей такого типа ($p\in \mathbf{N}$). *Степенью ненулевого многочлена и относительно* переменных X_ι, $\iota\in J$, назовем наибольшее из целых чисел p, для которого существует ненулевой член $a_{(n_\iota)}\prod_\iota X_\iota^{n_\iota}$ с $\sum_\iota n_\iota = p$. В частности, когда J состоит из одного элемента $\varkappa$, степень многочлена u относительно $X_\varkappa$ мы будем обозначать символом $\deg_\varkappa u$. Мы оставляем читателю возможность сформулировать с этими определениями предложения 2 и 3 для кольца $B[X_\iota]_{\iota\in J}$.

В кольце многочленов $A[X]$ от одной переменной имеется, естественно, только одно понятие степени. Однородные многочлены имеют вид λX^p ($\lambda\in A$). Ненулевой многочлен степени n записывается, как $u = \sum_{k=0}^{n} a_k X^k$. Коэффициент a_n, который, по предположению, отличен от нуля, называется *старшим коэффициентом* многочлена u. Ненулевой многочлен, старший коэффициент которого равен 1, называется *унитарным многочленом*.

Градуированные алгебры и модули. Понятие степени в алгебре многочленов есть частный случай более общего понятия, многочисленные примеры которого мы встретим позже.

Пусть A — коммутативное кольцо с единицей, E — алгебра над A, L — аддитивно записанный *коммутативный моноид*. *Градуировкой алгебры E со значениями в моноиде L* (или по моноиду L) называется семейство $(H_\lambda)_{\lambda\in L}$ *A-подмодулей алгебры E*, удовлетворяющее следующим условиям:

(AG_{I}) E есть *прямая сумма* H_λ;

(AG_{II}) $H_\lambda H_\mu \subset H_{\lambda+\mu}$.

Множество E, наделенное структурой алгебры и градуировкой (H_λ), назовем *градуированной алгеброй* (по L). Обычно мы будем говорить, что элементы из H_λ являются *однородными элементами степени* λ (или *веса* λ). Каждый элемент $x\in E$, в силу свойства (AG_{I}), однозначно записывается в виде $x=\sum_{\lambda\in L} x_\lambda$, где $x_\lambda\in H_\lambda$. Элемент x_λ называется однородной составляющей степени λ элемента x. Ненулевой однородный элемент x может принадлежать лишь к одному из модулей H_λ. Элемент $\lambda\in L$, для которого $x\in H_\lambda$, называется *степенью* (или *весом*) элемента x. Степень нулевого элемента не определяется. В большинстве случаев алгебра E будет обладать единицей, так что A можно отождествить с подалгеброй Ae алгебры E, моноид L будет обладать нейтральным элементом (мы обозначим его 0), и модуль H_0 отождествляется с A.

Градуировкой левого E-модуля M со значениями в L (или по L) называется семейство $(N_\lambda)_{\lambda\in L}$ A-подмодулей модуля M, удовлетворяющее условиям:

(MG_{I}) M есть *прямая сумма* подмодулей N_λ;

(MG_{II}) $H_\lambda N_\mu \subset N_{\lambda+\mu}$.

Говорят, что M, наделенный своей структурой E-модуля и градуировкой (N_λ), является *градуированным E-модулем* (по L). Понятия «однородный элемент модуля M» и «однородная составляющая элемента из M» определяются, как выше.

Примеры. 1) В алгебре многочленов $A[X_\iota]_{\iota\in I}$ подмодули однородных многочленов (соответственно однородных многочленов относительно переменных X_ι, $\iota\in I$) определяют градуировку этой алгебры по аддитивному моноиду $\boldsymbol{N}$. Степень в этой градуировке совпадает с полной степенью многочлена (соответственно степенью относительно переменных X_ι, $\iota\in J$), определенной выше.

2) Пусть теперь J и J' — два непересекающихся подмножества множества I. Для каждой пары натуральных чисел (p, q) определим $H_{p,q}$ как множество многочленов, однородных степени p относительно переменных X_ι, $\iota\in J$, и в то же время однородных степени q относительно переменных X_ι, $\iota\in J'$. Немедленно проверяется, что модули $H_{p,q}$ определяют градуировку алгебры $A[X_\iota]_{\iota\in I}$ по моноиду $\boldsymbol{N}\times\boldsymbol{N}$. Таким же образом определим градуировку $A[X_\iota]_{\iota\in I}$ по произведению произвольного числа (не превосходящего мощности множества I) моноидов, изоморфных $\boldsymbol{N}$.

3) Пусть M — произвольный коммутативный моноид, записанный аддитивно, с нейтральным элементом (обозначаемым символом 0). Пусть $(\omega_\iota)_{\iota\in I}$ — произвольное семейство элементов из M. Назовем *членами веса* ω ($\omega\in M$) в многочлене $u\in A[X_\iota]_{\iota\in I}$ члены $a_{(n_\iota)}\Pi X_\iota^{n_\iota}$, у которых $\sum_\iota n_\iota\omega_\iota=\omega$. Пусть H_ω — множество многочленов, у которых все ненулевые члены имеют вес ω. Немедленно проверяется, что H_ω определяют градуировку алгебры $A[X_\iota]_{\iota\in I}$ по моноиду M. Градуировку в примере 1 можно получить как частный случай этой общей градуировки.

4) В тензорной алгебре $T(E)$ (соответственно внешней алгебре $\bigwedge E$) произвольного A-модуля E обозначим для каждого $p\geqslant 0$ через H_p подмодуль, образованный контравариантными тензорами порядка p (соответственно p-векторами). Подмодули H_p определяют градуировку по моноиду $\mathcal{N}$.

5) Пусть L — коммутативный моноид (записанный аддитивно), E — *алгебра моноида* L относительно A (гл. II, § 7, n° 9) $(e_\lambda)_{\lambda\in L}$ — канонический базис E. В этом случае подмодули Ae_λ алгебры E (где λ пробегает L) образуют градуировку E по моноиду L.

4. *Многочлены над кольцом целостности*

Теорема 1. *Кольцо многочленов $A[X_\iota]_{\iota\in I}$ над кольцом целостности A* (с единицей) *является кольцом целостности.*

Пусть u, v — два многочлена из $A[X_\iota]_{\iota\in I}$. Три многочлена u, v и uv принадлежат одному и тому же кольцу $A[X_\iota]_{\iota\in\tau}$, где J — некоторое конечное подмножество множества I. Надо доказать, что если $u\neq 0$ и $v\neq 0$, то $uv\neq 0$. Таким образом, можно ограничиться рассмотрением случая, когда множество I конечно. С другой стороны, кольцо $A[X_1, X_2, \ldots, X_p]$ изоморфно кольцу многочленов от X_p с коэффициентами в кольце $A[X_1, \ldots, X_{p-1}]$. Следовательно, применением индукции по p задача сводится к доказательству теоремы для случая $p=1$, т. е. для кольца многочленов $A[X]$ от одной переменной над A.

Пусть $u=\alpha_0+\alpha_1X+\ldots+\alpha_mX^m$ — многочлен степени m, $v=\beta_0+\beta_1X+\ldots+\beta_nX^n$ — многочлен степени n над A; тогда коэффициент при X^{m+n} в произведении uv равен $\alpha_m\beta_n$. Так как $\alpha_m\neq 0$ и $\beta_n\neq 0$, по предположению, то ввиду того, что A — кольцо целостности, очевидно, имеем $\alpha_m\beta_n\neq 0$. Следовательно, $uv\neq 0$.

В общем случае, когда A содержит делители 0, предыдущее рассуждение показывает, что если старший коэффициент a_m многочлена u не является делителем 0 в A, то сам многочлен u не является делителем 0 в $A[X]$. В частности, это всегда имеет место в тех случаях, когда u — унитарный многочлен.

Следствие 1. *Пусть A — кольцо целостности, и u и v — два ненулевых многочлена из кольца $A[X_\iota]_{\iota\in I}$. В этом случае*

$$\deg(uv) = \deg u + \deg v. \tag{5}$$

Действительно, если $\deg u = m$, $\deg v = n$, то можно написать

$$u = u_0 + u_1 + \ldots + u_m, \quad v = v_0 + v_1 + \ldots + v_n,$$

где u_h (соответственно v_k) являются однородными составляющими степени h (соответственно k) многочлена u (соответственно v) для $0 \leqslant h \leqslant m$ (соответственно $0 \leqslant k \leqslant n$). Так как $u_m \neq 0$ и $v_n \neq 0$ по предположению, то $u_m v_n \neq 0$ по теореме 1. Следствие доказано ввиду того, что $u_m v_n$ является однородной составляющей степени $m+n$ многочлена uv.

Следствие 2. *Пусть A — кольцо целостности, и u и v — два ненулевых многочлена из кольца $A[X_\iota]_{\iota\in I}$. Для каждого $\varkappa \in I$ имеет место*

$$\deg_\varkappa(uv) = \deg_\varkappa u + \deg_\varkappa v. \tag{6}$$

5. *Евклидово деление многочленов одной переменной*

Предложение 4. *Пусть f — унитарный многочлен степени $n \geqslant 1$ в кольце $A[X]$. В факторалгебре $A[X]/(f)$ обозначим символом ξ класс, содержащий X. Тогда элементы* $1, \xi, \xi^2, \ldots, \xi^{n-1}$ *образуют базис алгебры $A[X]/(f)$.*

Докажем сначала, что элементы ξ^k $(0 \leqslant k \leqslant n-1)$ линейно независимы. Действительно, соотношение $\sum_{k=0}^{n-1} \lambda_k \xi^k = 0$ означает, что $\sum_{k=0}^{n-1} \lambda_k X^k \equiv 0 \pmod f$ или, иначе, что существует многочлен $g \in A[X]$, для которого $\sum_{k=0}^{n-1} \lambda_k X^k = fg$. В силу унитарности многочлена f имеем

$$\deg(fg) = \deg f + \deg g, \text{ если } g \neq 0;$$

так как степень многочлена f равна n, то предположение $g \neq 0$ приводит нас к противоречию. Следовательно, $\sum_{k=0}^{n-1} \lambda_k X^k = 0$. Таким образом, $\lambda_k = 0$ для $0 \leqslant k \leqslant n-1$.

Чтобы доказать, что элементы ξ^k *порождают* кольцо $A[X]/(f)$, достаточно показать для любого $p \geqslant 0$ сравнимость по модулю f многочлена X^p с нулевым многочленом или с многочленом степени $\leqslant n-1$. Проведем индукцию по p. Предложение очевидно для $p \leqslant n-1$. Если

$$X^p \equiv \sum_{k=0}^{n-1} \mu_k X^k \pmod{f}, \text{ то } X^{p+1} \equiv \sum_{k=0}^{n-2} \mu_k X^{k+1} + \mu_{n-1} X^n \pmod{f}.$$

Все сводится, таким образом, к доказательству предложения для $p = n$. Пусть $f = X^n + \sum_{n=1}^{n} \alpha_h X^{n-h}$; тогда $X^n \equiv -\sum_{h=1}^{n} \alpha_h X^{n-h} \pmod{f}$, чем и заканчивается доказательство.

Предложение 4 можно сформулировать и следующим образом:

Предложение 5. *Пусть f — унитарный многочлен степени n в кольце $A[X]$. Для любого многочлена $g \in A[X]$ существуют два многочлена u и v из $A[X]$ такие, что* $\deg v < n$ и

$$g = uf + v. \tag{7}$$

Кроме того, этими условиями многочлены u и v определяются однозначно.

Действительно, существование u и v и единственность v вытекают из предложения 4. С другой стороны, так как многочлен f не является делителем 0, то u однозначно определяется равенством (7).

Образование многочленов u и v, исходя из многочленов f и g, называется *евклидовым делением* многочлена g на f (по аналогии с *евклидовым делением* целых чисел (см. Теор. множ., гл. III и Алг., гл. I, § 4, n° 3). Многочлен u называется *евклидовым частным* от деления g на f, а многочлен v — *остатком* при евклидовом делении g на f.

Следствие. *Для того чтобы многочлен $g \in A[X]$ делился на унитарный многочлен $f \in A[X]$, необходимо и достаточно, чтобы остаток при евклидовом делении g на f был нулевым многочленом.*

Если A — поле, то предложение 5 справедливо и для произвольного ненулевого многочлена f. Действительно, пусть α_0 — старший коэффициент многочлена f; тогда идеалы (f) и $(\alpha_0^{-1}f)$ совпадают, причем $\alpha_0^{-1}f$ — унитарный многочлен. Следовательно, имеем

Предложение 6. *Пусть K — поле, f и g — два многочлена из кольца $K[X]$, причем $f \neq 0$. В этом случае существуют два многочлена u и v из $K[X]$ такие, что $\deg v < \deg f$ и имеет место соотношение* (7). *Кроме того, этими условиями многочлены u и v определяются единственным образом.*

Многочлены u и v называются также *частным* и *остатком* евклидового деления многочлена g на многочлен f.

Следствие. *Пусть A — кольцо целостности, K — его поле отношений, f и g — два многочлена из $A[X]$ степеней n и m соответственно. Пусть u и v — два многочлена из $K[X]$, удовлетворяющие равенству* (7), *причем $\deg v < n$. Положим $\mu = \operatorname{Max}(m-n+1, 0)$. Пусть α_0 — старший коэффициент многочлена f; тогда многочлены $\alpha_0^{\mu}u$ и $\alpha_0^{\mu}v$ принадлежат кольцу $A[X]$.*

Предложение очевидно для $m \leqslant n-1$, так как в этом случае $u=0$ и $v=g$. Для $m \geqslant n$ доказательство проведем индукцией по m. Достаточно рассмотреть случай $g = \beta X^m$. Пусть $f = \sum_{k=0}^{n} \alpha_k X^{n-k}$; имеем $\beta X^m = \frac{\beta}{\alpha_0} X^{m-n} f + \frac{1}{\alpha_0} g_1$, где многочлен $g_1 = -\sum_{k=1}^{n} \beta\alpha_k X^{m-k}$ принадлежит кольцу $A[X]$, причем $\deg g_1 \leqslant m-1$. По индуктивному предположению, $g_1 = u_1 f + v_1$, где $\deg v_1 < n$, а многочлены $\alpha_0^{m-n}u_1$ и $\alpha_0^{m-n}v_1$ принадлежат кольцу $A[X]$. Итак, имеем

$$\beta X^m = \frac{1}{\alpha_0}(u_1 + \beta X^{m-n}) f + \frac{1}{\alpha_0} v_1,$$

откуда тотчас вытекает следствие (ср. упражнение 12).

Предложение 7. *Пусть K — произвольное поле. Каждый идеал кольца многочленов одной переменной $K[X]$ над полем K является главным идеалом.*

Действительно, пусть $\mathfrak{a}$ — некоторый идеал в кольце $K[X]$. Если $\mathfrak{a} \neq (0)$, то пусть f — ненулевой элемент из $\mathfrak{a}$ наименьшей степени.

Пусть g — любой другой элемент из $\mathfrak{a}$. Можно написать: $g = uf + v$, где u и v — многочлены из $K[X]$, причем $v = 0$ или $\deg v < \deg f$ (предложение 6). Так как $v = g - uf$, то $v \in \mathfrak{a}$. Итак, в случае $v \neq 0$ мы получим $\deg v \geqslant \deg f$, что невозможно. Следовательно, $v = 0$. Это доказывает, что $\mathfrak{a} = (f)$.

Пусть f и f_1 — два ненулевых многочлена кольца $K[X]$, причем $(f) = (f_1)$. Тогда существуют два многочлена u и v такие, что $f = uf_1$ и $f_1 = vf$. Из этих соотношений получается равенство $f = uvf$, откуда следует, что $uv = 1$. Таким образом (формула (5)), u и v являются *константами*. Для любого ненулевого идеала $\mathfrak{a}$ в кольце $K[X]$ многочлены f, такие, что $\mathfrak{a} = (f)$, определяются с точностью до *постоянного множителя*. В частности, существует единственный *унитарный* многочлен f_0 такой, что $\mathfrak{a} = (f_0)$.

Пусть f и g — два многочлена из $K[X]$. Сумма $(f) + (g)$ главных идеалов, порожденных f и g, является главным идеалом (h) в силу предложенин 7. Для того чтобы многочлен u делил и f, и g, необходимо и достаточно, чтобы имели место включения $(u) \supset (f)$ и $(u) \supset (g)$, то есть $(u) \supset (f) + (g) = (h)$. Это означает, что u *делит* h. В случае $h \neq 0$ многочлен h, определяемый с точностью до постоянного множителя, является общим делителем многочленов f и g *наибольшей степени*. Мы назовем его также *наибольшим общим делителем* (сокращенно н. о. д.) многочленов f и g. Существуют два многочлена u и v из $K[X]$ такие, что выполняется равенство $h = uf + vg$. Говорят, что многочлены f и g *взаимно просты*, если $(h) = (1)$, т. е. если единственными общими делителями многочленов f и g являются константы, или, иначе, если существуют два многочлена u и v из $K(X)$, для которых $uf + vg = 1$. Пусть f и g — два произвольных многочлена из кольца $K[\alpha]$, h — их н. о. д. Если $h \neq 0$, то многочлены f/h и g/h взаимно просты. Обратно, это свойство характеризует н. о. д. многочленов f и g среди общих делителей этих многочленов. Эти замечания показывают, в частности, что, если h — н. о. д. многочленов f и g в кольце $K[X]$, то h является также н. о. д. многочленов f и g в кольце $K'[X]$, где K' — любое *поле*, содержащее K в качестве подполя.

Пересечение $(f) \cap (g)$ есть также главный идеал (r), где $r \in K[X]$. Аналогичные рассуждения показывают, что любое общее кратное многочленов f и g является кратным многочлена r. Если $r \neq 0$, то r является общим кратным наименьшей степени среди ненулевых общих кратных многочленов f и g. Мы назовем его наименьшим общим кратным (или кратко — н. о. к.) многочленов f и g.

Легко обобщить эти рассуждения на случай нескольких многочленов из кольца $K[X]$ (см. гл. VI, § 1, n° 8 и гл. VII, § 1, n° 2).

Определение 4. *Пусть K — поле. Назовем многочлен f ненулевой степени из кольца $K[X]$ неприводимым в $K[X]$ (или неприводимым над полем K), если он не делится ни на какой многочлен $g \in K[X]$, у которого $0 < \deg g < \deg f$.*

Равносильное условие (формула (5)) состоит в том, что единственными делителями многочлена f в кольце $K[X]$ являются константы и произведения f на константы. Так как соотношение $(f) \subset (g)$ означает, что g делит f, мы видим, что неприводимый многочлен можно определить как такой многочлен f, для которого идеал (f) *максимален*.

Известно (гл. I, § 8, теорема 2), что каждый идеал кольца $K[X]$, отличный от (1), *содержится в некотором максимальном идеале*. Исходя из предложения 7, можно сформулировать то же самое следующим образом.

Предложение 8. *Каждый многочлен, отличный от константы, в кольце $K[X]$ делится на некоторый неприводимый многочлен.*

Доказательство этого предложения можно провести, впрочем, и так: пусть f — произвольный ненулевой многочлен, отличный от константы, пусть g — делитель f, отличный от константы, причем наименьшей возможной степени. Немедленно получается, что g — неприводимый многочлен.

Следствие. *Каждый многочлен f положительной степени из кольца $K[X]$ равен произведению неприводимых многочленов (не обязательно различных).*

Достаточно провести индукцию по степени многочлена f. Утверждение следствия очевидно, если многочлен f неприводим. В противном случае существует неприводимый делитель g многочлена f, у которого $0 < \deg g < \deg f$. Имеем тогда $f = gh$, где $0 < \deg h < \deg f$. Поэтому многочлен h является произведением неприводимых многочленов. То же самое имеет место для многочлена f (мы уточним этот результат в гл. VI, § 1, n° 13 и в гл. VII, § 1, n° 3).

Упражнения. 1) Пусть A — коммутативное кольцо с единицей, E — некоторый A-модуль. Пусть $S_n(E)$ (или, проще, S_n) — подмодуль n-й тензорной степени $\overset{n}{\otimes} E$, порожденный тензорами вида $z - \sigma z$, где z пробегает $\overset{n}{\otimes} E$, а σ — симметрическую группу $\mathfrak{S}_n$ (см. гл. III, § 5). Назовем *n-й симметрической степенью* модуля E

и обозначим символом $\overset{n}{\bigvee} E$ фактормодуль $(\overset{n}{\bigotimes} E)/S_n(E)$. Для того чтобы полилинейное отображение модуля E^n в A-модуль F было симметрическим, необходимо и достаточно, чтобы оно имело вид: $(x_1, \ldots, x_n) \longrightarrow f(\varphi(x_1 \otimes \ldots \otimes x_n))$, где φ — каноническое отображение модуля $\overset{n}{\bigotimes} E$ на $\overset{n}{\bigvee} E$, f — некоторое линейное отображение модуля $\overset{n}{\bigvee} E$ в F.

Пусть E обладает базисом $(e_\iota)_{\iota \in I}$. Доказать, что *различные* элементы $\varphi(e_{\iota_1} \otimes e_{\iota_2} \otimes \ldots \otimes e_{\iota_n})$ образуют базис модуля $\overset{n}{\bigvee} E$ и что линейное отображение модуля $\overset{n}{\bigvee} E$ в A-модуль $A[X_\iota]_{\iota \in I}$, которое каждому элементу $\varphi(e_{\iota_1} \otimes e_{\iota_2} \otimes \ldots \otimes e_{\iota_n})$ ставит в соответствие одночлен $X_{\iota_1} X_{\iota_2} \ldots X_{\iota_n}$, является изоморфизмом модуля $\overset{n}{\bigvee} E$ на подмодуль H_n *однородных многочленов степени* n относительно X_ι.

Доказать, что в этом случае модуль $\overset{n}{\bigvee} E$ также изоморфен модулю симметрических контравариантных тензоров порядка n на E (установить взаимно однозначное соответствие между базисами этих двух модулей).

2) Доказать, что отображение $(z, z') \longrightarrow zz'$ модуля $(\overset{m}{\bigotimes} E) \times (\overset{n}{\bigotimes} E)$ в модуль $\overset{m+n}{\bigotimes} E$ согласуется с соотношениями эквивалентности по модулю S_m, по модулю S_n и по модулю S_{m+n} в модулях $\overset{m}{\bigotimes} E$, $\overset{n}{\bigotimes} E$ и $\overset{m+n}{\bigotimes} E$ соответственно. Переходя к фактормодулям, мы получим билинейное отображение, которое называется симметрическим произведением модуля $(\overset{m}{\bigvee} E) \times (\overset{n}{\bigvee} E)$ в модуль $\overset{m+n}{\bigvee} E$. Предположим, что E обладает базисом $(e_\iota)_{\iota \in I}$ и отождествим в этом случае модули $\overset{n}{\bigvee} E$, $\overset{m}{\bigvee} E$ и $\overset{m+n}{\bigvee} E$ с подмодулями H_m, H_n, H_{m+n} кольца $A[X_\iota]_{\iota \in I}$ (посредством изоморфизма, определенного в упражнении 1). Доказать, что симметрическое произведение отождествляется с произведением в кольце $A[X_\iota]_{\iota \in I}$.

3) Пусть S — оператор симметрии $\sum_{\sigma \in \mathfrak{S}_n} \sigma$ в тензорной степени $\overset{n}{\bigotimes} E$ (гл. III, § 5, п° 1; имеем, тем самым, $Sz = \sum_{\sigma \in \mathfrak{S}_n} \sigma z$). Для каждого тензора $z \in \overset{n}{\bigotimes} E$ элемент Sz симметричен и называется *симметризацией* тензора z. Доказать, что если в модуле E уравнение $n!\, x = a$ для каждого $a \in E$ допускает решение, и притом единственное, то каждый симметрический тензор n-го порядка на E является симметризацией некоторого тензора n-го порядка на E. Кроме того, взаимно однозначное представление, ассоциированное с линейным

отображением $z \longrightarrow Sz$ модуля $\overset{n}{\bigotimes} E$ в себя, является изоморфизмом модуля $\overset{n}{\bigvee} E$ на подмодуль симметрических тензоров.

Дать пример модуля E, у которого подмодуль симметрических тензоров и подмодуль симметризаций тензоров порядка n не совпадают (см. гл. III, § 4, упражнение 5).

4) Доказать, что если модуль E есть прямая сумма двух подмодулей E_1 и E_2, то симметрическая степень $\overset{n}{\bigvee} E$ изоморфна прямой сумме $Gn+1$ модулей $(\overset{p}{\bigvee} E_1) \otimes (\overset{n-p}{\bigvee} E_2)$, где $0 \leqslant p \leqslant n$ (методом упражнения 7 гл. III, § 5). Обобщить на случай, когда E является прямой суммой некоторого конечного числа подмодулей.

5) Пусть u — линейное отображение модуля E в модуль F, u_n — n-я тензорная степень отображения u. Имеет место включение $u_n(S_n(E)) \subset S_n(F)$. Переходя к фактормодулям, получим из u_n линейное отображение $\overset{n}{\bigvee} u$ модуля $\overset{n}{\bigvee} E$ в $\overset{n}{\bigvee} E$, называемое n-й симметрической степенью отображения u. Доказать, что если E и F — два векторных пространства над полем K и если u — линейное отображение конечного ранга r, то $\overset{n}{\bigvee} u$ является линейным отображением ранга $\binom{r+n-1}{n}$ (используя упражнение 11, гл. III, § 5).

6) Пусть E — алгебра над кольцом A, $(H_\lambda)_{\lambda \in L}$ — некоторая градуировка E по моноиду L. Пусть φ — некоторое представление моноида L в моноид M. Для каждого $\mu \in M$ обозначим символом H'_μ (прямую) сумму модулей H_λ, для которых $\varphi(\lambda) = \mu$. Доказать, что подмодули H'_μ образуют некоторую градуировку алгебры E по моноиду M.

7) Пусть E, F — две алгебры над кольцом A, $(H_\lambda)_{\lambda \in L}$ — некоторая градуировка алгебры E по моноиду L, (H'_μ) — градуировка алгебры F по моноиду M. Доказать, что подмодули $H_\lambda \otimes H'_\mu$ образуют градуировку тензорного произведения $E \otimes F$ по моноиду $L \times M$.

8) Пусть E — некоторая алгебра над кольцом A, $(H_\lambda)_{\lambda \in L}$ — градуировка алгебры E по моноиду L. Пусть $\mathfrak{a}$ — левый идеал (соответственно правый двусторонний) алгебры E, порожденный семейством *однородных* элементов (U_ι). Пусть C_λ — однородная составляющая идеала $\mathfrak{a}$ в H_λ. Доказать, что $\mathfrak{a}$ является прямой суммой подмодулей C_λ. Когда $\mathfrak{a}$ — двусторонний идеал, вывести отсюда, что канонические образы модулей H_λ в факторалгебре $E/\mathfrak{a}$ образуют градуировку этой алгебры по L.

*9) а) Пусть M — моноид, наделенный отношением порядка $x \leqslant y$, которое вполне упорядочивает M и для которого соотношения $x < y$, $x' \leqslant y'$ влекут $xTx' < yTy'$ (где T — обозначает закон композиции в M). Доказать, что если A кольцо целостности (с единицей), то алгебра моноида M относительно A является кольцом целостности.

°b) Обобщить евклидово деление многочленов одной переменной на случай алгебры группы M, где M является подгруппой аддитивной группы R действительных чисел.

10) Пусть A — кольцо целостности, f и g — два многочлена кольца $A[X_\iota]_{\iota\in I}$ такие, что fg — ненулевой однородный многочлен. Доказать, что f и g — однородные многочлены. В частности, доказать, что обратимые элементы кольца $A[X_\iota]_{\iota\in I}$ являются обратимыми элементами кольца A.

*11) Пусть A — произвольное коммутативное кольцо с единицей, $u=\sum_{k=0}^{m}\alpha_k X^k$ — делитель нуля в кольце $A[X]$. Доказать, что если $v=\sum_{k=0}^{n}\beta_k X^k$ — ненулевой элемент кольца $A[X]$ степени $h>0$, причем $uv=0$, то существует ненулевой многочлен w степени $n-1$ такой, что $uw=0$ (свести задачу к случаю, когда $\beta_0\neq 0$; если $\alpha_k v=0$ для $0\leqslant k\leqslant m-1$, то доказать, что можно положить $\omega=\beta_0$; если же $\alpha_k v=0$ для $0\leqslant k<p\leqslant m-1$ и $\alpha_p v\neq 0$, то доказать, что $\alpha_p\beta_0=0$, и, следовательно, можно положить $w=\sum_{k=0}^{n-1}\alpha_p\beta_{k+1}X^k$). Вывести отсюда, что в кольце A существует такой ненулевой элемент γ, что $\gamma u=0$.

12) Пусть A — коммутативное кольцо с единицей, f — ненулевой многочлен из кольца $A[X]$ степени n со старшим коэффициентом α_0. Пусть M — подмодуль в кольце $A[X]$ (рассматриваемом как A-модуль), образованный многочленами, у которых коэффициенты при члене степени m (m — произвольное натуральное число) делятся на α_0^{μ}, где $\mu=\mathrm{Max}(m-n+1, 0)$. Доказать, что для любого многочлена $g\in M$ найдутся два многочлена u и v из $A[X]$ такие, что $g=uf+v$, причем либо $v=0$, либо $\deg v<n$.

13) Пусть A — коммутативное кольцо с единицей, n — такое положительное целое число, что для всякого элемента $\alpha\in A$ в кольце A разрешимо уравнение $n\xi=\alpha$. Пусть m — некоторое целое положительное число и u — унитарный многочлен кольца $A[X]$ степени mn. Доказать, что в кольце $A[X]$ существует унитарный многочлен v степени m такой, что $u-v^n$ является либо нулевым многочленом, либо многочленом, степень которого $<mn-m$ (положить $v=X^m+w$).

§ 2. Полиномиальные функции

1. *Полиномиальные операторы*

Пусть A — *коммутативное* кольцо с единицей, E — алгебра с единицей над кольцом A, не обязательно коммутативная. Для каждого многочлена $f=\alpha_0+\alpha_1X+\ldots+\alpha_nX^n$ из кольца $A[X]$

многочленов одной переменной над кольцом A и каждого элемента $x \in E$ положим $f(x) = \alpha_0 e + \alpha_1 x + \ldots + \alpha_n x^n$.

Более общо. Пусть $\boldsymbol{x} = (x_\iota)_{\iota \in I}$ — некоторое семейство *попарно перестановочных* элементов алгебры E. Для каждого многочлена $f = \sum_{(n_\iota)} \alpha_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ из кольца $A[X_\iota]_{\iota \in I}$ положим $f(\boldsymbol{x}) = f((x_\iota)) = \sum_{(n_\iota)} \alpha_{(n_\iota)} \prod_{\iota \in I} x_\iota^{n_\iota}$. Будем говорить, что элемент $f(\boldsymbol{x})$ получен *подстановкой для каждого* $\iota \in I$ *элемента* x_ι *вместо переменной* X_ι *в многочлен* f.

Предложение 1. *Для всякого семейства* $\boldsymbol{x} = (x_\iota)_{\iota \in I}$ *попарно перестановочных элементов алгебры* E *отображение* $f \to f(x)$ *алгебры многочленов* $A[X_\iota]_{\iota \in I}$ *в алгебру* E *является представлением. Образом алгебры* $A[X_\iota]_{\iota \in I}$ *при этом представлении является* (коммутативная) *подалгебра алгебры* E, *порожденная множеством, состоящим из единичного элемента* e *и элементов* x_ι ($\iota \in I$).

Пусть f и g — два элемента из $A[X_\iota]_{\iota \in I}$, α — элемент из A. Положим $h_1 = f + g$, $h_2 = \alpha f$ и $h_3 = fg$. Надо доказать, что

$$h_1(\boldsymbol{x}) = f(\boldsymbol{x}) + g(\boldsymbol{x}), \quad h_2(\boldsymbol{x}) = \alpha f(\boldsymbol{x}) \quad \text{и} \quad h_3(\boldsymbol{x}) = f(\boldsymbol{x})\, g(\boldsymbol{x}).$$

Первые два соотношения очевидны. В силу формулы дистрибутивности в алгебре E достаточно доказать третью формулу в случае, когда f и g — одночлены. В этом случае формула следует из определения произведения двух одночленов и предположения о попарной перестановочности элементов x_ι. Образ алгебры $A[X_\iota]_{\iota \in I}$ при представлении $f \to f(\boldsymbol{x})$ является подалгеброй алгебры E, содержащей e и x_ι. С другой стороны, любая подалгебра алгебры E, содержащая эти элементы, содержит также и все элементы вида $f(\boldsymbol{x})$. Следовательно, множество элементов вида $f(\boldsymbol{x})$, когда f пробегает $A[X_\iota]_{\iota \in I}$, является, очевидно, подалгеброй алгебры E, порожденной множеством, являющимся объединением $\{e\}$ и множества M элементов x_ι.

Будем обозначать эту подалгебру символом $A[\boldsymbol{x}]$ или $A[x_\iota]_{\iota \in I}$, или еще $A[M]$.

Если I — конечное подмножество из $\boldsymbol{N}$ (наиболее часто встречающийся случай) и $(i_k)_{1 \leqslant k \leqslant p}$ — элементы из I, расположенные в строго возрастающей последовательности, то чаще всего вместо $f((x_\iota))$

и $A[x_\iota]_{\iota\in I}$ пишут

$$f(x_{i_1}, x_{i_2}, \ldots, x_{i_p}) \quad \text{и} \quad A[x_{i_1}, x_{i_2}, \ldots, x_{i_p}].$$

Из предложения 1 вытекает следующая

Теорема 1. *Пусть E — алгебра с единицей e над A, и пусть $x=(x_\iota)_{\iota\in I}$ — некоторое множество попарно перестановочных элементов из E. Подалгебра $A[x]$ алгебры E, порожденная элементом e и x_ι, изоморфна факторалгебре $A[X_\iota]_{\iota\in I}/\mathfrak{a}$, где $\mathfrak{a}$ — идеал алгебры $A[X_\iota]_{\iota\in I}$, образованный многочленами f, для которых $f(x)=0$.*

Идеал $\mathfrak{a}$ назовем (для краткости) *идеалом алгебраических соотношений с коэффициентами из кольца A между элементами x_ι* (или *алгебраических соотношений, которым удовлетворяет элемент x*, когда множество (x_ι) состоит из единственного элемента x). Он совпадает с модулем *линейных* соотношений с коэффициентами из кольца A между элементами $\prod_{\iota\in I} x_\iota^{n_\iota}$ (где (n_ι) пробегает $\mathbf{N}^{(I)}$) (гл. II, § 1, n° 8). Вообще говоря, этот идеал состоит не только из нуля. Следовательно, представление $f\to f(x)$ не является изоморфизмом алгебры $A[X_\iota]_{\iota\in I}$ на алгебру $A[x]$.

° Например, в кольце $C[X]$ многочленов одной переменной над полем C комплексных чисел многочлен $f=X^2+1$ отличен от нуля, но $f(i)=0$.

Предложение 2. *Пусть A, A' — изоморфные коммутативные кольца, обладающие единицей, φ — изоморфизм кольца A на кольцо A'. Пусть E* (соответственно E') *— алгебра с единицей e* (соответственно e') *над кольцом A* (соответственно A'), *и пусть $x=(x_\iota)_{\iota\in I}$* (соответственно $x'=(x'_\iota)_{\iota\in I}$) *— семейство попарно перестановочных элементов алгебры E* (соответственно E'), *$\mathfrak{a}$* (соответственно $\mathfrak{a}'$) *— идеал алгебраических соотношений между x_ι* (соответственно x'_ι). *Для того чтобы существовал изоморфизм ψ алгебры $A[x]$ на алгебру $A'[x']$ такой, что $\psi(x_\iota)=x'_\iota$ для любого $\iota\in I$ и $\psi(\alpha e)=\varphi(\alpha)e'$ для всякого α из A, необходимо и достаточно, чтобы выполнялось соотношение $\overline{\varphi}(\mathfrak{a})=\mathfrak{a}'$, где $\overline{\varphi}$ означает изоморфизм алгебры $A[X_\iota]_{\iota\in I}$ на $A'[X_\iota]_{\iota\in I}$, который продолжает φ и оставляет инвариантными X_ι* (§ 1, предложение 1). *Изоморфизм ψ, удовлетворяющий предыдущим условиям, при этом единственный.*

Действительно, если существует такой изоморфизм ψ, то для каждого многочлена $f \in \mathfrak{a}$, имеем $f(x)=0$, откуда, положив $\bar{f}=\bar{\varphi}(f)$, получим $\bar{f}(x')=0$, то есть $\bar{f} \in \mathfrak{a}'$. Следовательно, должно выполняться включение $\bar{\varphi}(\mathfrak{a}) \subset \mathfrak{a}'$. Применяя те же рассуждения к изоморфизму, обратному к ψ, получим включение $\overline{\varphi^{-1}}(\mathfrak{a}') \subset \mathfrak{a}$, откуда $\bar{\varphi}(\mathfrak{a})=\mathfrak{a}'$. Обратно, если это условие выполнено, то существует изоморфизм кольца $A[X_\iota]_{\iota \in I}/\mathfrak{a}$ на кольцо $A'[X_\iota]_{\iota \in I}/\mathfrak{a}'$, который смежному классу по идеалу $\mathfrak{a}$, порожденному элементом u кольца $A[X_\iota]_{\iota \in I}$, ставит в соответствие смежный класс по идеалу $\mathfrak{a}'$, порожденный элементом $\bar{\varphi}(u)$. В частности, классу (по идеалу $\mathfrak{a}$), порожденному элементом $\alpha \in A$, соответствует класс (по идеалу $\mathfrak{a}'$), порожденный элементом $\varphi(\alpha)$, а классу (по идеалу $\mathfrak{a}$), порожденному элементом X_ι, соответствует класс (по идеалу $\mathfrak{a}'$), порожденный элементом X_ι. Существование изоморфизма ψ вытекает из теоремы 1. Его единственность следует немедленно из вида элементов в $A'[x']$.

Замечания. 1) Известно, что любое кольцо E можно рассматривать как алгебру над кольцом Z целых рациональных чисел (с законом композиции $(n, x) \to nx$; см. гл. II, § 7, n° 1).

Теорема 1 описывает, следовательно, структуру подколец кольца E (без операторов, или, что то же самое, рассматриваемых как алгебра над Z), порожденных единичным элементом в E и каким-нибудь семейством попарно перестановочных элементов кольца E.

2) Отметим, что для применения теоремы 1 не обязательно, чтобы отображение $\alpha \to \alpha e$ кольца A в алгебру E было изоморфизмом. Например, пусть E—алгебра над Z; может оказаться, что $nx=0$ для всех $x \in E$ и некоторого ненулевого целого числа n (в случае, если характеристика алгебры E отлична от нуля и делит n).

3) Отображение $(f, x) \to f(x)$ из $A[X] \times E$ в E является *внешним законом композиции* на алгебре E с кольцом $A[X]$ в качестве кольца операторов. Предложение 1 доказывает, что этот закон дистрибутивен, с одной стороны, по отношению к двум аддитивным законам на $A[X]$ и E и, с другой стороны, по отношению к двум мультипликативным законам на этих же кольцах (см. гл. I, § 5, n° 1). Многочлен X является нейтральным оператором при этом внешнем законе. Наконец, если ограничиться множеством операторов из подкольца A кольца $A[X]$, мы опять получим внешний закон композиции в алгебре E.

4) Если в алгебре E отсутствует единичный элемент, то можно определить $f(x)$ для любого семейства $x=(x_\iota)_{\iota \in I}$ попарно переста-

новочных элементов из E и любого многочлена $f \in A[X_\iota]_{\iota \in I}$ *без свободного члена*. Пусть B — подалгебра алгебры $A[X_\iota]_{\iota \in I}$, образованная такими многочленами; тогда отображение $f \to f(X)$ алгебры B в алгебру E является представлением и образ алгебры B при этом представлении является подалгеброй в алгебре E, порожденной множеством элемеятов x_ι.

2. *Подстановка многочленов в многочлен*

Если алгебра E *коммутативна*, то можно, очевидно, подставлять в многочлен $f \in A[X_\iota]_{\iota \in I}$ вместо всякого X_ι произвольный элемент x_ι из E. Рассмотрим, в частности, случай, когда E является *алгеброй многочленов* $A[Y_\lambda]_{\lambda \in L}$. Для любого семейства $(g_\iota)_{\iota \in I}$ многочленов этой алгебры можно тогда определить многочлен $h = f((g_\iota))$ (принадлежащий к $A[Y_\lambda]_{\lambda \in L}$), полученный подстановкой g_ι вместо X_ι. Пусть F — алгебра с единичным элементом над A, $y = (y_\lambda)_{\lambda \in L}$ — семейство попарно перестановочных элементов из F. Легко видеть, что имеет место тождество $h(y) = f((g_\iota(y)))$ в случае, когда f — одночлен (предложение 1).

Более частный случай: можно взять в качестве E ту же алгебру $A[X_\iota]_{\iota \in I}$. Это позволяет, в частности, пользоваться записью $f = f((X_\iota))$ (или $f = f(X_1, X_2, \ldots, X_n)$ для многочленов от n переменных), подставляя X_ι вместо самих себя для всех ι.

Предложение 3. *Для всякого многочлена $f \in A[X_\iota]_{\iota \in I}$ и любого семейства $(a_\iota)_{\iota \in I}$ элементов кольца A свободный член многочлена $h = f((X_\iota + a_\iota))$ равен $f((a_\iota))$.*

Действительно, подставив 0 вместо каждого из X_ι в многочлене h, в силу предыдущих замечаний мы получим требуемое утверждение.

Следствие. *Каждый многочлен $f \in A[X, Y]$, для которого $f(X, X) = 0$, делится на $X - Y$.*

Действительно, в многочлене от Z вида $g(X, Z) = f(X, X+Z)$ с коэффициентами в кольце $A[X]$ свободный член равен $f(X, X) = 0$. Поэтому существует многочлен $h(X, Z) \in A[X, Z]$ такой, что $g(X, Z) = Zh(X, Z)$, откуда, подставляя $Y - X$ вместо Z, получим $f(X, Y) = (Y - X)h(X, Y - X)$.

Предложение 4. *Для всякого многочлена $f \in A[X_\iota]_{\iota \in I}$ его однородная часть f_k степени k равна коэффициенту при члене*

Z^k *в многочлене* $f((X_\iota Z))$ (рассматриваемом как многочлен от Z с коэффициентами в кольце $A[X_\iota]_{\iota \in I}$).

Достаточно доказать это для одночлена. В этом случае предложение следует немедленно.

Следствие. *Для того чтобы некоторый многочлен* $f \in A[X_\iota]_{\iota \in I}$ *был однородным многочленом степени* k, *необходимо и достаточно, чтобы имело место равенство*

$$f((X_\iota Z)) = f((X_\iota))\, Z^k. \tag{1}$$

3. Полиномиальные функции на алгебре

Пусть A — коммутативное кольцо с единицей, E — алгебра над A с единичным элементом e (не предполагаем, что представление $\alpha \to \alpha e$ из A в E является изоморфизмом). Для каждого многочлена $f \in A[X]$ и для любого элемента $x \in E$ определено выражение $f(x)$. Отображение $x \to f(x)$ является отображением из E в E. Мы назовем его *полиномиальной функцией*, ассоциированной с многочленом f.

Предположим теперь, что алгебра E, кроме того, *коммутативна*. Пусть I — произвольное множество индексов, f — некоторый многочлен из алгебры $A[X_\iota]_{\iota \in I}$; значение $f(x)$ определено тогда для каждого семейства $x = (x_\iota)_{\iota \in I}$ элементов из E, имеющего I в качестве множества индексов. Отображение $x \to f(x)$ является, следовательно, отображением из E^I в E, которое мы также называем *полиномиальной функцией*, ассоциированной с многочленом f. Полиномиальная функция, определенная на E^I, является, следовательно, отображением вида $(x_\iota) \to \sum_{(n_\iota)} a_{(n_\iota)} \prod x_\iota^{n_\iota}$, где (n_ι) пробегает $\mathbf{N}^{(I)}$, а $a_{(n_\iota)}$ равны нулю всюду, за исключением конечного числа элементов из $\mathbf{N}^{(I)}$.

Например, любая *линейная форма* на A-модуле A^n (гл. II, § 4, n° 1) записывается в виде $(x_1, \ldots, x_n) \to \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$, где α_i принадлежат кольцу A. Она является, следовательно, полиномиальной функцией, ассоциированной с однородным многочленом первой степени $\alpha_1 X_1 + \ldots + \alpha_n X_n$ (откуда название «линейная форма», которое для краткости применяется к однородным одночленам первой степени; см. § 1, n° 3).

Таким же образом, если каждой «двойной последовательности» (x_{ij}) $(1 \leqslant i \leqslant n;\ 1 \leqslant j \leqslant n)$ элементов произвольного коммутативного

кольца E (без операторов) поставить в соответствие определитель $\det(x_{ij})$ квадратной матрицы (x_{ij}), то мы определим полиномиальную функцию, ассоциированную с многочленом $\sum_{\sigma \in \sigma_n} \varepsilon_\sigma X_{1,\sigma(1)} \times \times X_{2,\sigma(2)} \cdots X_{n,\sigma(n)}$, то есть с многочленом $\det(X_{ij})$ в кольце $Z[X_{11}, \ldots, X_{nn}]$ многочленов над кольцом Z относительно n^2 переменных X_{ij}.

Для любого многочлена f из алгебры $A[X_\iota]_{\iota \in I}$ обозначим символом $\tilde{f}$ полиномиальную функцию $x \to f(x)$, которая ему соответствует (отображение из E^I в E). По предложению 1 отображение $f \to \tilde{f}$ является *представлением* алгебры $A[X_\iota]_{\iota \in I}$ в алгебру отображений из E^I в E. Мы вскоре увидим в n° 4 и 5, что это представление не всегда является *изоморфизмом* (иначе говоря, одна и та же полиномиальная функция может быть ассоциирована с несколькими различными многочленами, то есть может существовать такой ненулевой многочлен f, что $f(x) = 0$ для *каждого* $x \in E^I$). Попутно мы получим достаточные условия для того, чтобы отображение $f \to \tilde{f}$ являлось изоморфизмом.

Даже когда представление $f \to \tilde{f}$ не является изоморфизмом, отображение $x \to f(x)$ часто обозначают символом f, допуская вольность речи. Никакой путаницы не произойдет в том случае, если при введении элемента f уточнять, идет ли речь *о многочлене* f или *о полиномиальной функции* f.

4. Корни многочлена от одной переменной

Пусть даны многочлен $f \in A[X_\iota]_{\iota \in I}$ и коммутативная алгебра E (с единицей) над A. Говорят, что элемент $x = (x_\iota)$ множества E^I является *нулем многочлена* f в E^I, если $f(x) = 0$. Если f — многочлен относительно одной переменной X, то нуль x многочлена f в E называют также *корнем* многочлена f в E.

Мы сначала рассмотрим корни многочлена $f \in A[X]$, *которые принадлежат кольцу* A (рассматриваемому как алгебра над самим собой).

Предложение 5. *Для того чтобы элемент* $\alpha \in A$ *был корнем многочлена* $f \in A[X]$, *необходимо и достаточно, чтобы* $X - \alpha$ *был делителем многочлена* f *в кольце* $A[X]$.

Действительно, свободный член многочлена $f(\alpha+Y)$ равен $f(\alpha)$ (предложение 3). Для справедливости равенства $f(\alpha)=0$ необходимо и достаточно, очевидно, чтобы многочлен $f(\alpha+Y)$ делился на Y. Отсюда следует предложение, так как достаточно подставить $X-\alpha$ вместо Y.

Если элемент $\alpha\in A$ является корнем ненулевого многочлена $f\in A[X]$, то f может делиться на степень $(X-\alpha)^h$ многочлена $(X-\alpha)$ с показателем степени $h>1$. Так как $(X-\alpha)^h$ — унитарный многочлен, то он не является делителем нуля в кольце $A[X]$. Поэтому соотношение $f=(X-\alpha)^h g$ однозначно определяет многочлен g и $\deg f=h+\deg g$. Тем самым можно ввести следующее определение:

Определение 1. *Назовем порядком кратности корня $\alpha\in A$ ненулевого многочлена $f\in A[X]$ наибольшее из чисел h таких, что $(X-\alpha)^h$ делит f. Корень, порядок кратности которого равен k, называется кратным корнем порядка k.*

Кратный корень порядка 1 называется *простым* корнем. Кратный корень порядка 2 (соответственно 3, 4, ...) называется *двойным* (соответственно *тройным*, *четырехкратным*, ...).

Для того чтобы элемент $\alpha\in A$ являлся корнем порядка k многочлена f, необходимо и достаточно, чтобы имело место равенство $f=(X-\alpha)^k g$, где g не делится на $X-\alpha$. Действительно, это условие, очевидно, необходимо. Оно и достаточно, так как, если бы элемент α был корнем порядка $h>k$, то многочлен g делился бы на $(X-\alpha)^{h-k}$, ибо многочлен $(X-\alpha)^k$ не является делителем нуля в кольце $A[X]$. По предложению 5, это условие равносильно неравенству $g(\alpha)\neq 0$. Так как $\deg f=k+\deg g$, имеет место соотношение $k\leqslant\deg f$.

Замечания. 1) Для всякого ненулевого многочлена $f\in A[X]$ распространим определение 1 на все элементы $\alpha\in A$, условясь считать нулем *порядок кратности элемента α относительно многочлена f*, если α не является корнем этого многочлена.

2) Утверждение, что порядок кратности элемента $\alpha\in A$ относительно ненулевого многочлена f не меньше h, означает, что многочлен $(X-\alpha)^h$ *делит* f. Для нулевого многочлена 0 порядок кратности какого бы то ни было элемента кольца A не определен. Но, допуская вольность речи, условимся говорить, сверх того, что порядок кратности элемента $\alpha\in A$ относительно *произвольного* многочлена f не меньше h в том случае, когда многочлен $(X-\alpha)^h$ делит f.

3) Пусть B — некоторое подкольцо кольца A, f — многочлен кольца $B[X] \subset A[X]$, α — элемент из B, который является корнем многочлена f. Тогда порядок кратности элемента α относительно многочлена f *не зависит* от того, рассматривать многочлен f как элемент кольца $B[X]$ или как элемент кольца $A[X]$. Действительно, соотношения $(X-\alpha)^h g(X) = (X-\alpha)^k g_1(X)$, где $g \in A[X]$, $g_1 \in B[X]$ и $g(\alpha) \neq 0$, $g_1(\alpha) \neq 0$, возможны лишь в случае $h = k$, так как многочлен $X - \alpha$ не является делителем нуля в кольце $A[X]$.

Предложение 6. *Пусть f и g — два ненулевых многочлена из кольца $A[X]$, α — произвольный элемент кольца A, p и q — порядки кратности α относительно f и g соответственно.*

1° *Порядок кратности α относительно многочлена $f+g$ не меньше* $\operatorname{Min}(p, q)$. *Если $p \neq q$, то он равен* $\operatorname{Min}(p, q)$.

2° *Порядок кратности α относительно многочлена fg не меньше $p+q$. Если A — кольцо целостности, то этот порядок равен $p+q$*

Действительно, имеем $f(X) = (X-\alpha)^p f_1(X)$, $g(X) = (X-\alpha)^q g_1(X)$ с $f_1(\alpha) \neq 0$ и $g_1(\alpha) \neq 0$. Пусть, скажем, $p \leqslant q$. Тогда $f(X) + g(X) = (X-\alpha)^p (f_1(X) + (X-\alpha)^{q-p} g_1(X))$, и если $p < q$, то α не является корнем многочлена $f_1(X) + (X-\alpha)^{q-p} g_1(X)$, что доказывает первую часть предложения. Вторая вытекает таким же образом из формулы $f(X) g(X) = (X-\alpha)^{p+q} f_1(X) g_1(X)$ и из того, что $f_1(\alpha) g_1(\alpha) \neq 0$, если A — кольцо целостности.

Предложение 7. *Пусть A — кольцо целостности* (с единицей), *f — ненулевой многочлен из $A[X]$. Пусть α_i $(1 \leqslant i \leqslant p)$ — p различных корней многочлена f в A, порядки кратностей которых суть k_i $(1 \leqslant i \leqslant p)$. В этом случае многочлен f делится на*

$$(X-\alpha_1)^{k_1} (X-\alpha_2)^{k_2} \dots (X-\alpha_p)^{k_p}.$$

Будем вести индукцию по p. В силу определения 1 предложение очевидно для случая, когда $p = 1$. Пусть имеет место соотношение

$$f(X) = (X-\alpha_1)^{k_1} (X-\alpha_2)^{k_2} \dots (X-\alpha_{p-1})^{k_{p-1}} g(X), \qquad (2)$$

где $g \in A[X]$. Элемент α_p является корнем порядка k_p многочлена f и не является корнем многочлена $\prod_{i=1}^{p-1} (X-\alpha_i)^{k_i}$ (так как, по предположению, $\alpha_i - \alpha_p \neq 0$ для $1 \leqslant i \leqslant p-1$ и A есть кольцо

целостности). Из предложения 6 вытекает, что α_p является корнем порядка k_p многочлена g. Следовательно, многочлен g делится на $(X-\alpha_p)^{k_p}$. Отсюда следует предложение.

Теорема 2. *Пусть A — кольцо целостности* (с единицей), *f — многочлен из $A[X]$ степени $\leqslant h$. Если $f \neq 0$, то сумма порядков кратностей всех корней многочлена f в A не превосходит n. В частности, если полиномиальная функция $\tilde{f}$, определенная в A, аннулируется $n+1$ различными значениями переменной, то $f=0$.*

Это непосредственное следствие предложения 7.

Следствие. *Пусть A — кольцо целостности, f и g — два многочлена из $A[X]$, степень которых $\leqslant n$. Если значения полиномиальных функций $\tilde{f}$ и $\tilde{g}$, определенных на A, совпадают при $n+1$ различных значениях переменной, то $f=g$.*

Достаточно применить теорему 2 к многочлену $f-g$.

Замечания. 1) Теорема 2 неверна в случае, когда кольцо A обладает делителями нуля. Например, в кольце $Z/(16)$ многочлен X^2 имеет *четыре* различных корня, а именно смежные классы (по модулю 16), порожденные элементами 0, 4, 8, 12.

2) Пусть A — поле с бесконечным числом элементов, E — алгебра над A с единицей, которую можно отождествить с единичным элементом поля A (так что поле A отождествляется с подполем центра алгебры E). В этом случае ненулевой многочлен из $A[X]$ может иметь только *конечное число* корней *в* A (по теореме 1). Но он может иметь *бесконечное число их в* алгебре E. Например, если a и b — два элемента алгебры E, линейно независимые относительно A и такие, что $a^2=ab=ba=b^2=0$, то все элементы вида $a+\lambda b$, где λ пробегает A, являются нулями в E многочлена X^2 (упражнение 7 и гл. VIII, § 11, упражнение 7).

Приложение. *Интерполяционная формула Лагранжа.* Пусть K — некоторое поле, α_i $(1 \leqslant i \leqslant n)$ — n различных элементов из поля K, β_i $(1 \leqslant i \leqslant n)$ — n каких-либо (различных или нет) элементов поля K. Зададимся целью определить многочлены $f \in K[X]$ такие, что $f(\alpha_i)=\beta_i$ для $1 \leqslant i \leqslant n$. Речь идет о системе линейных скалярных уравнений в векторном пространстве $K[X]$ (гл. II, § 4, n° 7).

Соответствующая линейная однородная система ($\beta_i=0$ для $1 \leqslant i \leqslant n$) имеет в качестве решения, в силу предложения 7, многочлен

$$f(X)=(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)\,g(X),$$

где g — *произвольный* многочлен из $K[X]$. Нам достаточно, следовательно, иметь одно решение системы, чтобы получить все решения (гл. II, § 4, предложение 11). Предположим сначала, что $\beta_k = 1$ и $\beta_i = 0$ для $i \neq k$. Любой искомый многочлен делится тогда, согласно предложению 7, на произведение $(X-\alpha_1)\ldots(X-\alpha_{k-1})(X-\alpha_{k+1})\ldots(X-\alpha_n)$. Докажем, что можно найти такой скаляр $\lambda \in K$, что многочлен $u_k(X) = \lambda(X-\alpha_1)\ldots(X-\alpha_{k-1})(X-\alpha_{k+1})\ldots(X-\alpha_n)$ является решением нашей задачи. Действительно, условие $u_k(\alpha_k) = 1$ дает

$$\lambda(\alpha_k-\alpha_1)\ldots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\ldots(\alpha_k-\alpha_n) = 1,$$

откуда можно определить λ потому, что разность $\alpha_k - \alpha_i$, по предположению, отлична от нуля для $i \neq k$. Определив таким образом многочлены u_k для $1 \leqslant k \leqslant n$, вернемся к общему случаю, где β_i произвольные. Непосредственно видно, что многочлен $f = \sum_{i=1}^{n} \beta_i u_i$ отвечает нашей задаче, причем либо $f = 0$, либо степень f не превосходит $n-1$. Очевидно, что это *единственное* решение, обладающее этим свойством (следствие теоремы 2). Найденное выражение

$$f(X) = \sum_{i=1}^{n} \beta_i \frac{(X-\alpha_1)\ldots(X-\alpha_{i-1})(X-\alpha_{i+1})\ldots(X-\alpha_n)}{(\alpha_i-\alpha_1)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_n)}$$

называется *интерполяционной формулой Лагранжа.*

5. *Полиномиальные функции на кольце целостности с бесконечным числом элементов*

Предложение 8. *Пусть A — кольцо целостности* (с единицей) *с бесконечным множеством элементов. Пусть H_i $(1 \leqslant i \leqslant n)$ — n бесконечных частей кольца A. Для любого ненулевого многочлена $f \in A[X_1, X_2, \ldots, X_n]$ существует бесконечно много элементов $X = (x_1, x_2, \ldots, x_n)$ множества $\coprod_{i=1}^{n} H_i$, для которых $f(X) \neq 0$.*

Ввиду теоремы 2 предложение справедливо при $n = 1$. Будем вести доказательство индукцией по n. Многочлен f можно рассматривать как многочлен относительно X_n с коэффициентами

в кольце $A[X_1, X_2, \ldots, X_{n-1}]$. Пусть $f = \sum_{k=0}^{m} g_k X_n^k$. Так как $f \neq 0$, то по крайней мере один из коэффициентов $g_i \in A[X_1, \ldots, X_{n-1}]$ отличен от нуля. В силу предположения индукции существует система $(x_1, x_2, \ldots, x_{n-1}) \in \prod_{i=1}^{n-1} H_i$, для которой $g_i(x_1, \ldots, x_{n-1}) \neq 0$. Из этого следует, что многочлен $h(X_n) = \sum_{k=0}^{m} g_k(x_1, \ldots, x_{n-1}) X_n^k$ кольца $A[X_n]$ отличен от нуля. По теореме 2 существует бесконечно много элементов $x_n \in H_n$ таких, что $h(x_n) \neq 0$. Так как $h(x_n) = f(x_1, \ldots, x_{n-1}, x_n)$, то предложение доказано.

Предложение 9. *Пусть A — кольцо целостности с бесконечным множеством элементов; тогда отображение $f \to \tilde{f}$ алгебры многочленов $A[X_\iota]_{\iota \in I}$ в алгебру отображений из A^I в A является изоморфизмом.*

Действительно, пусть f — ненулевой многочлен из $A[X_\iota]_{\iota \in I}$. Существует конечная часть J множества I такая, что f принадлежит кольцу $A[X_\iota]_{\iota \in J}$. По предложению 8 существует такой элемент $y = (y_\iota)_{\iota \in J}$ множества A^J, что для любого элемента $x = (x_\iota)_{\iota \in I}$ из A^I, проекция которого на A^J есть y, имеет место неравенство $f(x) \neq 0$. Отсюда следует предложение.

Другими словами, если для любого элемента $x = (x_\iota) \in A^I$ имеет место тождество $\sum_{(n_\iota)} a_{(n_\iota)} \prod_\iota x_\iota^{n_\iota} = 0$, то $a_{(n_\iota)} = 0$ для каждого $(n_\iota) \in N^{(I)}$.

Когда A — кольцо целостности с бесконечным множеством элементов (случай, наиболее часто встречающийся в приложениях), изоморфизм $f \to \tilde{f}$ позволяет *отождествить* кольцо $A[X_\iota]_{\iota \in I}$ с кольцом соответствующих полиномиальных функций.

Допуская обычную вольность речи, которая заключается в смешении *функции* и ее *значения* на общем элементе области определения (Теор. § 2, n° 2), мы будем говорить в таких случаях о «многочлене $f(x)$» или о «многочлене $a_0 + a_1 x + \ldots + a_n x^n$». Пока и поскольку сформулированные ранее условии выполнены, этот язык не представляет никаких неудобств.

Замечания. 1) Пусть E — такая коммутативная алгебра с единицей над A, что A можно отождествить с подалгеброй Ae

алгебры E. Если A — бесконечное кольцо целостности, то отображение $f \to \tilde{f}$ из $A[X_\iota]_{\iota \in I}$ в алгебру отображений множества E^I в E по-прежнему является *изоморфизмом*, так как для любого ненулевого многочлена $f \in A[X_\iota]_{\iota \in I}$ существует элемент $x \in A^I \subset E^I$, для которого $f(x) \neq 0$. Когда речь идет о многочленах от одной переменной, можно не предполагать коммутативности алгебры E (см. упражнение 13).

2) В формулировке предложения 8 на кольцо A были наложены два условия:

1° целостность, 2° бесконечность. Результат перестает быть верным, если предположить, что A удовлетворяет *лишь одному* из этих условий (упражнения 8 и 9). Однако эти два условия *не являются необходимыми* для того, чтобы отображение $f \to \tilde{f}$ из $A[X_\iota]_{\iota \in I}$ в алгебру отображений множества A^I в A было изоморфизмом (упражнение 6).

Теорема 3 (принцип продолжения алгебраических тождеств). *Пусть A — бесконечное кольцо целостности с единицей, (g_i) $(1 \leqslant i \leqslant m)$ — конечная последовательность ненулевых многочленов из $A[X_1, X_2, \ldots, X_n]$. Пусть f — такой многочлен из $A[X_1, X_2, \ldots, X_n]$, что $f(x_1, x_2, \ldots, x_n) = 0$ для любого элемента $(x_j) \in A^n$, для которого $g_i(x_1, x_2, \ldots, x_n) \neq 0$ при всех $1 \leqslant i \leqslant m$ тогда $f = 0$.*

Действительно, если $f \neq 0$, то многочлен $h = fg_1g_2 \ldots g_n$ отличен от нуля (§ 1, теорема 1), следовательно (предложение 8), существует элемент $(x_j) \in A^n$, для которого $h(x_1, x_2, \ldots, x_n) \neq 0$, что противоречит предположению.

Схолия. Теорема 3 дает очень удобное средство для доказательства того, что некоторый многочлен f относительно n переменных над кольцом целостности A (с единицей) равен нулю. Достаточно рассмотреть *бесконечное* кольцо целостности E, содержащее подкольцо, изоморфное кольцу A и имеющее тот же самый единичный элемент, что и E. Если мы докажем, что $f(x_1, x_2, \ldots, x_n) = 0$ для всех элементов $(x_i) \in E^n$ (или только для тех элементов из E^n, которые не аннулируют некоторое конечное число фиксированных ненулевых полиномиальных функций), то отсюда будет следовать, что $f = 0$. Если кольцо A само бесконечно, то можно взять в качестве E само кольцо A или поле частных кольца A. В противном случае можно, например,

взять в качестве E кольцо $A[X]$ многочленов от одной переменной над A (или его поле частных).

Доказав соотношение $f=0$, очевидно, из него можно вывести равенства $f(y_1, y_2, \ldots, y_n)=0$ для любого элемента $(y_i)\in F^n$, где F — *произвольная* коммутативная алгебра над A (с единицей e). Алгебра F может иметь, в частности, лишь конечное число элементов или иметь делители 0. При этом отображение $a \to ae$ из A в F может не быть взаимно однозначным.

Другими словами, доказательство тождеств $f(x_1, x_2, \ldots, x_n)=0$, когда x_i пробегают *бесконечное кольцо целостности, содержащее A, и с той же самой единицей, что у A* (возможно, с ограничением типа $g_i(x_1, \ldots, x_n)\neq 0$ для $1\leqslant i\leqslant m$, где g_i — некоторые ненулевые многочлены), влечет *те же тождества*, когда x_i пробегают *произвольную коммутативную алгебру* (с единицей) над A.

В частности, если многочлен f относительно n переменных с *целыми рациональными* коэффициентами таков, что $f(x_1, x_2, \ldots, x_n)=0$, когда x_i пробегают *поле рациональных чисел* Q (возможно, с ограничением типа $g_i(x_1, x_2, \ldots, x_n)\neq 0$, где g_i — ненулевые многочлены с целыми коэффициентами), то имеет место то же самое тождество, когда x_i пробегают *какое бы то ни было коммутативное кольцо* с единицей (даже когда это кольцо имеет характеристику >0), так как принцип продолжения алгебраических тождеств показывает, что $f=0$ в кольце $Z[X_1, X_2, \ldots, X_n]$.

Упражнения. *1) а) В алгебре $A[X]$ многочленов от одной переменной над кольцом A отображение $(u, v)\to u(v)$ является внутренним законом композиции. Доказать, что этот закон ассоциативен и дистрибутивен слева относительно сложения и умножения в алгебре $A[X]$.

б) Доказать, что если A — кольцо целостности, то из соотношения $u(v)=0$ следует, что либо $u=0$, либо v является константой. Кроме того, если $u\neq 0$ и $\deg v>0$, то степень многочлена $u(v)$ равна произведению степеней многочленов u и v.

в) Будем предполагать в дальнейшем, что A *поле*. Пусть u и v — многочлены из кольца $A[X]$, степень которых >0, f — многочлен степени >0. Доказать, что если q и r — соответственно частное и остаток при евклидовом делении многочлена u на v, то $q(f)$ и $r(f)$ являются частным и остатком при евклидовом делении многочлена $u(f)$ на $v(f)$.

г) Для любого многочлена f из кольца $A[X]$ обозначим символом $I(f)$ множество многочленов вида $u(f)$, где u пробегает $A[X]$. Это — подкольцо кольца $A[X]$. Для того чтобы кольца $I(f)$ и $I(g)$

совпадали, необходимо и достаточно, чтобы имело место тождество вида $g=\lambda f+\mu$, где $\lambda \neq 0$ и μ — элементы кольца A.

д) Пусть f и g — два многочлена положительной степени в кольце $A[X]$. Доказать, что пересечение $I(f)\cap I(g)$ либо совпадает с A, либо имеет вид $I(h)$, где h — некоторый многочлен положительной степени (исключая первую возможность, рассмотреть в кольце $I(f)\cap I(g)$ многочлен h наименьшей положительной степени; заметить затем, что любой многочлен $u \in A[X]$ однозначно записывается в виде $\sum_h v_h h^k$, где $v_h=0$ или $\deg v_h < \deg h$, и что если $u \in I(f)$, то v_h также принадлежат $I(f)$; использовать в)).

*2) Пусть K — поле, $K[X]$ — кольцо многочленов над K от одной переменной. Доказать, что любой автоморфизм s кольца (без операторов) $K[X]$ оставляет инвариантным поле K (см. § 1, упражнение 10) и индуцирует на K некоторый автоморфизм σ_s этого поля. Кроме того, доказать, что $s(X)=\lambda X+\mu$, где $\lambda \neq 0$ и μ — элементы полн K (использовать упражнение 1б)). Обратно, доказать, что задание произвольного автоморфизма σ поля K и двух элементов λ и μ из полн K ($\lambda \neq 0$) однозначно определяет автоморфизм S кольца $K[X]$, для которого $\sigma_s=\sigma$ и $s(X)=\lambda X+\mu$. Пусть G — группа всех автоморфизмов кольца $K[X]$ без операторов, H — подгруппа группы G, состоящая из автоморфизмов структуры *алгебры* $K[X]$ над полем K; доказать, что подгруппа H отлична от G и группа G/H изоморфна группе автоморфизмов поля K. Группа H изоморфна группе, определенной на множестве $K^*\times K$ законом композиции

$$(\lambda,\ \mu)\ (\lambda',\ \mu')=(\lambda\lambda',\ \lambda'\mu+\mu').$$

3) Пусть A — кольцо целостности, f — многочлен из кольца $A[X_1, X_2, \ldots, X_n]$ степени $\leqslant k_i$ относительно X_i (для $1 \leqslant i \leqslant n$). Для любого значения индекса i ($1 \leqslant i \leqslant n$) пусть H_i — множество из k_i+1 элементов кольца A. Доказать, что если $f(x_1, x_2, \ldots, x_n)=0$ при всех $(x_i) \in \prod_{i=1}^{n} H_i$, то $f=0$.

4) Пусть A — кольцо целостности с бесконечным числом элементов, Φ — множество ненулевых многочленов из кольца $A[X_1, X_2, \ldots, X_n]$. Доказать, что если мощность множества Φ *строго меньше* мощности кольца A, то существует часть H в A^n, равномощная с A и такая, что для любых $X=(x_i) \in H$ и $f \in \Phi$ имеет место неравенство $f(X) \neq 0$.

5) Пусть A — бесконечное кольцо целостности, B — бесконечная часть кольца A. Доказать, что если многочлен $f \in A[X]$ имеет положительную степень, то образ B относительно полиномиального отображения $x \to f(x)$ имеет одинаковую мощность с B.

6) Пусть A — коммутативное кольцо с единицей, у которого существует бесконечная подгруппа G аддитивной группы A, все

элементы которой не являются делителями нуля в A. Доказать, что отображение $f \to \tilde{f}$ из $A[X_1, \ldots, X_p]$ в алгебру отображений множества A^p в A является изоморфизмом. (Заметить, что многочлен степени n относительно одной переменной не может иметь более чем n различных корней, принадлежащих G.) Так обстоит дело, в частности, когда в кольце A существует элемент x_0, не являющийся делителем нуля, порядок которого в аддитивной группе A бесконечен.

7) Пусть K — бесконечное поле, характеристика которого отлична от двух. Пусть Q — алгебра кватернионов над K, соответствующая паре $(-1, -1)$ (гл. II, § 7, n° 8). Доказать, что многочлен X^2+1 имеет бесконечно много нулей в Q.

*8) Пусть K — конечное поле из q элементов.

а) Пусть $\mathfrak{a}$ — идеал в кольце $K[X_1, X_2, \ldots, X_n]$, порожденный n многочленами $X_i^q - X_i$ $(1 \leqslant i \leqslant n)$. Доказать, что если $f \in \mathfrak{a}$, то имеет место равенство $f(x_1, x_2, \ldots, x_n)=0$ для всех $(x_i) \in K^n$ (заметить, что мультипликативная группа K^* имеет порядок $q-1$).

б) Пусть f — произвольный многочлен из кольца $K[X_1, X_2, \ldots, X_n]$. Доказать, что существует единственный многочлен $\bar{f}$, либо равный нулю, либо такой, что $\deg_i \bar{f} \leqslant q-1$ для всех $1 \leqslant i \leqslant n$, причем $f \equiv \bar{f} \pmod{\mathfrak{a}}$. Имеет место неравенство $\deg \bar{f} \leqslant \deg f$. Пусть f — многочлен, для которого $f(x_1, x_2, \ldots, x_n)=0$ при всех $(x_i) \in K^n$; тогда f принадлежит идеалу $\mathfrak{a}$, который является, таким образом, прообразом нуля при представлении $f \to \tilde{f}$ (использовать упражнение 3).

в) Пусть $f_1, f_2, \ldots, f_m$ — ненулевые многочлены из кольца $K[X_1, X_2, \ldots, X_n]$, причем $f_i(0, 0, \ldots, 0)=0$ $(1 \leqslant i \leqslant m)$ и сумма полных степеней многочленов f_i строго меньше n. Доказать, что существует такой элемент $(x_1, x_2, \ldots, x_n) \in K^n$, отличный от $(0\ 0, \ldots, 0)$, что

$$f_i(x_1, x_2, \ldots, x_n)=0 \quad \text{для} \quad 1 \leqslant i \leqslant m. \bullet$$

(Заметить, что если бы это было не так, то многочлен $\prod_{i=1}^{m} (1-f_i^{q-1})$ находился бы в одном смежном классе по модулю $\mathfrak{a}$ с многочленом $\prod_{j=1}^{n} (1-X_j^{q-1})$. Использовать б).)

9) Пусть K — конечное поле, имеющее q элементов, A — кольцо K^I, являющееся произведением I экземпляров поля K, где I — бесконечное множество. Привести пример ненулевого многочлена f из $A[X]$ такого, что $f(x)=0$ для любого $x \in A$.

10) Обобщить упражнения 10—14 гл. III, § 8 на случай, когда квадратные матрицы, рассматриваемые в этих упражнениях, не имеют обратных.

11) В кольце многочленов от 8 переменных X_i, Y_i $(1 \leqslant i \leqslant 4)$ над кольцом Z целых рациональных чисел. Установить соотношение

$$(X_1^2+X_2^2+X_3^2+X_4^2)(Y_1^2+Y_2^2+Y_3^2+Y_4^2)=$$
$$=(X_1Y_1-X_2Y_2-X_3Y_3-X_4Y_4)^2+(X_1Y_2+X_2Y_1+X_3Y_4-X_4Y_3)^2+$$
$$+(X_1Y_3+X_3Y_1+X_4Y_2-X_2Y_4)^2+(X_1Y_4+X_4Y_1+X_2Y_3-X_3Y_2)^2$$

(использовать тот факт, что в алгебре кватернионов над полем Q рациональных чисел, соответствующей паре $(-1, -1)$ (гл. II, § 7, n° 8), норма произведения равна произведению норм сомножителей).

12) Доказать, что в кольце многочленов от 6 переменных X_i, Y_i $(1 \leqslant i \leqslant 3)$ над Z не существуют соотношения вида $(X_1^2+X_2^2+X_3^2) \times (Y_1^2+Y_2^2+Y_3^2)=u^2+v^2+w^2$, где u, v, w — три многочлена относительно X_i и Y_i с целыми коэффициентами. (Заметить, что число $15=3\cdot 5$ нельзя представить в виде $m^2+n^2+p^2$, где m, n, p — целые.)

13) Пусть E — кольцо целостности с бесконечным числом элементов, с единицей e, наделенное структурой алгебры относительно кольца целостности A (с единицей). Пусть $\mathfrak{a}$ — идеал кольца A, являющийся аннулятором e (для структуры E как A-модуля). Доказать, что если $A_1=A/\mathfrak{a}$, то образ кольца $A[X_1, X_2, \ldots, X_n]$ при отображении $f \to \tilde{f}$ в кольцо отображений множества E^n в E изоморфен кольцу $A_1[X_1, X_2, \ldots, X_n]$.

§ 3. Рациональные дроби и рациональные функции

1. Рациональные дроби над полем

Определение 1. *Пусть K — поле. Рациональными дробями с коэффициентами из K относительно переменных X_ι $(\iota \in I)$ называются элементы поля отношений* (гл. I, § 9, n° 4) *кольца целостности $K[X_\iota]_{\iota \in I}$ многочленов с коэффициентами из K относительно переменных X_ι.*

Поле рациональных дробей с коэффициентами из K относительно X_ι обозначается символом $K(X_\iota)_{\iota \in I}$, когда I — интервал $[1, n]$ из $\mathbf{N}$, поле $K(X_i)_{i \in I}$ обозначают также символом $K(X_1, X_2, \ldots, X_n)$ и называют *полем рациональных дробей от n переменных* с коэффициентами из K.

По определению поля отношений кольца целостности, каждая рациональная дробь поля $K(X_\iota)_{\iota \in I}$ может быть представлена бесконечным множеством способов в виде $\frac{u}{v}$, где u и v — два многочлена из кольца $K[X_\iota]_{\iota \in I}$, причем $v \neq 0$. Соотношение

$\frac{u}{v} = \frac{u_1}{v_1}$ ($v \neq 0$, $v_1 \neq 0$) означает, что $uv_1 = vu_1$. Таким образом, если $u \neq 0$, то и $u_1 \neq 0$. В этом случае (§ 1, формула (5)) $\deg u + \deg v_1 = \deg v + \deg u_1$ или еще $\deg u_1 - \deg v_1 = \deg u - \deg v$. Целое число (положительное или отрицательное) $\deg u - \deg v$ не зависит, тем самым, от представления ненулевой рациональной дроби в виде частного $\frac{u}{v}$ двух многочленов. Это число называется (*полной*) *степенью* этой дроби. Таким же образом определяют *степень* ненулевой рациональной дроби *относительно переменной* $X_\varkappa$. Тотчас же проверяется, что для многочленов с коэффициентами из K эти понятия совпадают с одноименными понятиями, определенными в § 1, и что формулы (3), (5) и (6) § 1 остаются справедливыми для степеней рациональных дробей.

Замечание. Если A—кольцо целостности с единицей, то, как известно (§ 1, теорема 1), кольцо $A[X_\iota]_{\iota \in I}$ также является кольцом целостности. Пусть K—поле отношений кольца A. Можно отождествить K с подполем отношений кольца $A[X_\iota]_{\iota \in I}$, состоящим из дробей $\frac{u}{v}$, где u и v—многочлены нулевой степени ($v \neq 0$), отождествленные с элементами кольца A. При этом соглашении поле отношений кольца $A[X_\iota]_{\iota \in I}$ отождествляется с полем рациональных дробей $K(X_\iota)_{\iota \in I}$. Действительно, каждый многочлен из $K[X_\iota]_{\iota \in I}$ можно записать в виде $\frac{u}{a}$, где u—многочлен с коэффициентами из A, a—элемент кольца A (достаточно привести к общему знаменателю все коэффициенты рассматриваемого многочлена). Каждая рациональная дробь из $K(X_\iota)_{\iota \in I}$ записывается, следовательно, в виде $(u/\alpha)/(v/\beta) = (\beta u)/(\alpha v)$, где α и β принадлежат A, а u и v—кольцу $A[X_\iota]_{\iota \in I}$. Тем самым эта дробь является элементом поля отношений кольца $A[X_\iota]_{\iota \in I}$.

Пусть теперь K—произвольное поле, J—непустая часть множества индексов I. Мы видели (§ 1, n° 2), что кольцо многочленов $K[X_\iota]_{\iota \in I}$ можно отождествить с кольцом многочленов относительно переменных X_ι (индекс $\iota \in CJ$) с коэффициентами из кольца целостности $B = K[X_\iota]_{\iota \in J}$. Предыдущее замечание доказывает, что можно отождествить поле рациональных дробей $K(X_\iota)_{\iota \in I}$ с полем рациональных дробей относительно X_ι, $\iota \in CJ$, с коэффициентами из поля рациональных дробей $K(X_\iota)_{\iota \in J}$.

Предложение 1 из § 1 вместе с предложением 4 из гл. I, § 9 показывает, что имеет место

Предложение 1. *Пусть K, K' — два изоморфных поля, φ — изоморфизм K на K'. В этом случае существует изоморфизм $\bar{\varphi}$, и притом единственный, поля $K(X_\iota)_{\iota\in I}$ на $K'(X_\iota)_{\iota\in I}$, который продолжает φ и оставляет инвариантным каждую переменную X_ι.*

2. Рациональные дроби, рассматриваемые как операторы

Пусть A — коммутативная алгебра с единицей над полем K, причем единица алгебры отождествлена с единицей поля K. Пусть $f=\frac{u}{v}$ — элемент поля $K(X_\iota)_{\iota\in I}$. Пусть $x=(x_\iota)_{\iota\in I}$ — элемент множества A^I, для которого значение $v(x)$ обратимо в кольце A; тогда элемент $\frac{u(x)}{v(x)}$ определен в кольце A. Кроме того, если u_1 и v_1 — другие многочлены, для которых $f=\frac{u_1}{v_1}$, причем значение $v_1(x)$ также обратимо, то $\frac{u(x)}{v(x)}=\frac{u_1(x)}{v_1(x)}$. Это следует из того, что $uv_1=u_1v$, и, значит, $u(x)v_1(x)=u_1(x)v(x)$ (§ 2, предложение 1). Если существует *по крайней мере одно* представление дроби f в виде $\frac{u}{v}$, где $v(x)$ — обратимый элемент, то мы будем говорить, что семейство $x=(x_\iota)$ *допускает подстановку* в рациональную дробь f. Мы только что видели, что для всех представлений дроби f в виде частного $\frac{u}{v}$ двух многочленов, для которых $v(x)$ — обратимый элемент, элемент $\frac{u(x)}{v(x)}$ кольца A оказывается одним и тем же. Мы будем обозначать его символом $f(x)$ или $f((x_\iota))$.

Предложение 2. *Пусть $x=(x_\iota)_{\iota\in I}$ — произвольное семейство элементов коммутативной алгебры A над полем K. Множество рациональных дробей $f\in K(X_\iota)_{\iota\in I}$, для которых x допускает подстановку, образует подалгебру U поля $K(X_\iota)_{\iota\in I}$. Отображение $f\to f(x)$ является представлением алгебры U в A. Образ подалгебры U при этом отображении совпадает со множеством элементов вида yz^{-1}, где y пробегает кольцо $K[x]$, а z — множество обратимых элементов этого кольца.*

В самом деле, пусть $f_1=\frac{u_1}{v_1}$, $f_2=\frac{u_2}{v_2}$ — две рациональные дроби, для которых $v_1(x)$ и $v_2(x)$ являются обратимыми элементами. В этом случае имеют место тождества $f_1+f_2=\frac{u_1v_2+u_2v_1}{v_1v_2}$ и $f_1f_2=\frac{u_1u_2}{v_1v_2}$. Положим $v=v_1v_2$; тогда $v(x)=v_1(x)v_2(x)$ — обратимый элемент. Таким образом, U является подалгеброй. Учитывая предложение 1 из § 2, мы немедленно убеждаемся, что отображение $f\to f(x)$ является представлением алгебры U в A. Заключительное утверждение предложения очевидно.

Следствие. *Пусть K_0 — поле, являющееся расширением поля K, U — подкольцо кольца $K(X_\iota)_{\iota\in I}$, образованное рациональными дробями f, для которых семейство $x=(x_\iota)\in K_0^I$ допускает подстановку в f; тогда образ кольца U при отображении $f\to f(x)$ является подполем поля K_0, порожденным объединением K и множества M элементов x_ι $(\iota\in I)$.*

Действительно, из вышесказанного и предложения 6 гл. I, § 9 следует, что этот образ изоморфен полю отношений кольца $K[x]$. Мы будем обозначать это подполе символом $K(x)$ или $K(x_\iota)_{\iota\in I}$ (или еще $K(x_1, x_2, \ldots, x_n)$, когда $I=[1, h]$), а иногда также символом $K(M)$.

3. Подстановка рациональной дроби в рациональную дробь

Рассмотрим, в частности, следствие предложения 2 для случая, когда поле K_0 есть *поле рациональных дробей* $K(Y_\lambda)_{\lambda\in L}$. Пусть $(g_\iota)_{\iota\in I}$ — семейство элементов этого поля, допускающих подстановку в рациональную дробь $f\in K(X_\iota)_{\iota\in I}$; тогда значение $f((g_\iota))=h$ является рациональной дробью относительно Y_λ. Кроме того, справедливо

Предложение 3. *Пусть f — рациональная дробь из поля $K(X_\iota)_{\iota\in I}$, $(g_\iota)_{\iota\in I}$ — семейство элементов поля рациональных дробей $K(Y_\lambda)_{\lambda\in L}$, $y=(y_\lambda)_{\lambda\in L}$ — семейство элементов поля K. Предположим, что семейство y допускает подстановку в каждую из дробей g_ι, а семейство элементов $(g_\iota(y))_{\iota\in I}$ — подстановку в дробь f. В этом случае семейство элементов (g_ι) допускает подстановку в f. Если положить $h=f((g_\iota))$, то семейство $y=(y_\lambda)$ допускает подстановку в h, причем $h(y)=f((g_\iota(y)))$.*

Очевидно, можно предположить, что множества I и L *конечны*. В силу предположений можно представить g_ι в виде $\frac{p_\iota}{q_\iota}$, где p_ι и q_ι — многочлены из кольца $K[Y_\lambda]_{\lambda\in L}$, причем $q_\iota(\boldsymbol{y}) \neq 0$ для всех $\iota \in I$. Таким же образом можно написать: $f = \frac{u}{v}$, где u, v — такие многочлены из кольца $K[X_\iota]_{\iota\in I}$, что $v((g_\iota(\boldsymbol{y}))) \neq 0$. Пусть m — наивысшая из степеней многочленов u и v относительно каждой переменной X_ι. Пусть w — многочлен из $K[Y_\lambda]_{\lambda\in L}$, являющийся произведением многочленов q_ι ($\iota \in I$). В этом случае $u_1 = w^m u((g_\iota))$ и $v_1 = w^m v((g_\iota))$ являются многочленами из $K[Y_\lambda]_{\lambda\in L}$, причем $v_1(\boldsymbol{y}) = (w(\boldsymbol{y}))^m v((g_\iota(\boldsymbol{y}))) \neq 0$. Следовательно, $v_1 \neq 0$ и $v((g_\iota)) \neq 0$. Таким образом, семейство (g_ι) допускает подстановку в f и имеет место равенство $h = f((g_\iota)) = \frac{u_1}{v_1}$. Тем самым y допускает подстановку в h и $h(\boldsymbol{y}) = f((g_\iota(\boldsymbol{y})))$.

В частности, семейство $(X_\iota)_{\iota\in I}$ допускает подстановку в *любую* рациональную дробь $f \in K(X_\iota)_{\iota\in I}$. Поэтому можно писать $f = f((X_\iota))$ (или — для рациональных дробей от n переменных — $f = f(X_1, X_2, \ldots, X_n)$).

4. *Рациональные функции*

Пусть K — поле, K_0 — расширение поля K, причем с *бесконечным* множеством элементов. Для любой рациональной дроби $f \in K(X_\iota)_{\iota\in I}$ обозначим символом S_f часть множества K_0^I, образованную семействами $\boldsymbol{x} = (x_\iota)_{\iota\in I}$, допускающими подстановку в f. В силу предложения 8 из § 2 множество S_f *бесконечно*. *Рациональной функцией*, ассоциированной с рациональной дробью f (со значениями в расширении K_0 поля K) назовем отображение $\boldsymbol{x} \to f(\boldsymbol{x})$ из множества S_f в поле K_0. Мы будем обозначать это отображение символом $\tilde{f}$ (или просто f, если исключена возможность путаницы). Пусть f и g — две рациональные дроби из $K(X_\iota)_{\iota\in I}$; тогда множество $S_f \cap S_g$ непусто (§ 2, теорема 3). Если для любого элемента $\boldsymbol{x}$ этого множества имеет место равенство $f(\boldsymbol{x}) = g(\boldsymbol{x})$, то $f = g$ Действительно, пусть $f = \frac{u}{v}$, $g = \frac{u_1}{v_1}$. В силу принципа продолжения алгебраических тождеств (§ 2, теорема 3) из равенства $u(\boldsymbol{x})v_1(\boldsymbol{x}) = u_1(\boldsymbol{x})v(\boldsymbol{x})$, справедливого для всех

$x=(x_\iota)$, для которых $v(x)\neq 0$ и $v_1(x)\neq 0$, следует, что $uv_1=u_1v$. Другими словами, отображение $f\to\tilde{f}$ *взаимно однозначно.*

Заметим теперь, что любой элемент множества $S_f\cap S_g$ (f и g — произвольные рациональные дроби из $K(X_\iota)_{\iota\in I}$) допускает подстановку в дробь $f+g$ (fg соответственно). Таким образом, рациональная функция, ассоциированная с $f+g$ (fg соответственно), определена и принимает те же значения, что и функция $\tilde{f}+\tilde{g}$ (соответственно $\tilde{f}\tilde{g}$) на множестве $S_f\cap S_g$. Аналогично для ненулевой рациональной функции f образуем часть S'_f в K_0^I из элементов x, допускающих подстановку в f, причем $f(x)\neq 0$. Множество S'_f непусто (§ 2, теорема 3). Рациональная дробь $1/f$ определена и принимает те же значения, что и функция $1/\tilde{f}$ на каждом элементе x множества S'_f.

Замечания. 1) Позднее мы увидим, что для любой ненулевой рациональной дроби f существуют два таких многочлена u_0 и v_0, что $f=\frac{u_0}{v_0}$ и множество элементов S_f, допускающих подстановку в f, совпадает с множеством элементов x, для которых $v_0(x)\neq 0$.

2) Принцип продолжения алгебраических тождеств (§ 2, теорема 3) можно распространить на рациональные дроби. Пусть f и g_i $(1\leqslant i\leqslant m)$ — рациональные дроби из $K(X_\iota)_{\iota\in I}$, причем $g_i\neq 0$. Предположим, что для любого семейства $x\in K_0^I$, допускающего одновременно подстановку в f и во все g_i и такого, что $g_i(x)\neq 0$ для $1\leqslant i\leqslant m$, имеет место равенство $f(x)=0$. В этом случае $f=0$ (поле K_0 всегда предполагается бесконечным). Это предложение немедленно вытекает из теоремы 3 § 2.

Упражнения. 1) Пусть A — коммутативная алгебра с единицей над полем K, $x=(x_\iota)_{\iota\in I}$ — элемент множества A^I. Пусть U — подкольцо в $K(X_\iota)_{\iota\in I}$, состоящее из тех элементов $f\in K(X_\iota)_{\iota\in I}$, для которых x допускает подстановку в f. Доказать, что если в алгебре A необратимые элементы образуют идеал, то этот факт имеет место и в кольце U. Доказать, что в случае, когда A — поле, являющееся расширением поля K, необратимые элементы в кольце U образуют максимальный идеал.

2) а) Пусть $u=a_mX^m+a_{m+1}X^{m+1}+\ldots+a_nX^n$ — многочлен из $K[X]$, у которого $a_m\neq 0$ и $a_n\neq 0$ $(0\leqslant m\leqslant n)$. Доказать, что для всякой рациональной дроби g ненулевой степени d поля $K(X)$ дробь $u(g)$ отлична от нуля и имеет степень nd, если $d>0$, и степень md, если $d<0$.

б) Вывести, что рациональная дробь g из $K(X)$, отличная от константы, допускает подстановку в любую рациональную дробь из

$K(X)$. (Заметить, что если степень дроби g равна нулю, то существует такой элемент $a \in K$, что $g-a$ уже имеет степень строго меньшую нуля.)

3) Рациональная дробь $f \in K(X_1, X_2, \ldots, X_n)$ называется *однородной*, если она равна частному двух однородных многочленов (с ненулевым знаменателем). Доказать, что рациональная дробь f однородна в том и только в том случае, когда

$$f(ZX_1, ZX_2, \ldots, ZX_n) = Z^d f(X_1, \ldots, X_n),$$

где d — степень f.

§ 4. Дифференциалы и дифференцирования

1. Дифференциалы и производные многочленов

Мы ограничимся в этом параграфе рассмотрением многочленов и рациональных дробей от *конечного* числа переменных над произвольным коммутативным кольцом A (с единицей).

Пусть f — некоторый многочлен из кольца $A[X_1, X_2, \ldots, X_p] = B$. Рассмотрим многочлен $f(X_1+Y_1, X_2+Y_2, \ldots, X_p+Y_p)$ в кольце многочленов $A[X_1, \ldots, X_p, Y_1, \ldots, Y_p]$ от $2p$ переменных X_i, Y_i $(1 \leqslant i \leqslant p)$. Этот многочлен можно рассматривать как многочлен относительно Y_i с коэффициентами в кольце B. Как таковой, он имеет свободный член, равный $f(X_1, X_2, \ldots, X_p)$ (§ 2, предложение 3). Положим

$$\Delta f = f(X_1+Y_1, \ldots, X_p+Y_p) - f(X_1, \ldots, X_p).$$

Таким образом, многочлен Δf (который иногда обозначают символом $\Delta f(X_1, \ldots, X_p; Y_1, \ldots, Y_p)$) является многочленом без свободного члена из кольца $B[Y_1, Y_2, \ldots, Y_p]$.

Определение 1. *Назовем дифференциалом многочлена f и обозначим символом df или $df(X_1, \ldots, X_p; Y_1, \ldots, Y_p)$ однородную часть первой степени многочлена Δf, рассматриваемого как многочлен относительно переменных Y_i с коэффициентами в кольце $B = A[X_1, X_2, \ldots, X_p]$.*

Согласно этому определению можно написать

$$df = \sum_{i=1}^{p} g_i Y_i, \tag{1}$$

где $g_1, g_2, \ldots, g_n$ — элементы кольца B, то есть многочлены из кольца $A[X_1, X_2, \ldots, X_p]$.

Определение 2. *Назовем частной производной многочлена f относительно переменной X_i $(1 \leqslant i \leqslant p)$ и обозначим символом $D_i f$* $\left(\text{или } D_{X_i} f, \text{ или } \frac{\partial f}{\partial X_i}, \text{ или } f'_{X_i}\right)$ *многочлен из кольца $B = A[X_1, X_2, \ldots, X_p]$, являющийся коэффициентом при Y_i в дифференциале df многочлена f.*

Таким образом, формула (1) запишется в виде

$$df = \sum_{i=1}^{p} (D_i f)\, Y_i = \sum_{i=1}^{p} \frac{\partial f}{\partial X_i} Y_i. \tag{2}$$

В частном случае, когда $f = X_i$ имеем $df = Y_i$. Это позволяет, допуская некоторую вольность, пользоваться записью переменных Y_i в виде dX_i $(1 \leqslant i \leqslant p)$ и приводит к формуле

$$df = \sum_{i=1}^{p} (D_i f)\, dX_i = \sum_{i=1}^{p} \frac{\partial f}{\partial X_i} dX_i. \tag{3}$$

Если f — многочлен относительно одной переменной, то $df = Df \cdot dX$. Многочлен Df $\left(\text{который обозначают также символом } \frac{\partial f}{\partial X} \text{ или } f'\right)$ в этом случае называют просто *производной* от f.

Если f — константа, то, очевидно, $\Delta f = 0$. Следовательно, $df = 0$.

Обращение этого предложения неверно: если A — кольцо характеристики $q > 0$, то производная многочлена X^q равна $qX^{q-1} = 0$ (следствие 3 предложения 1).

Предложение 1. *Пусть f и g — два многочлена из кольца*

$$B = A[X_1, X_2, \ldots, X_p].$$

Тогда

$$d(f + g) = df + dg, \tag{4}$$

$$d(fg) = df \cdot g + f \cdot dg. \tag{5}$$

Формула (4) немедленно следует из определения 1. Для доказательства соотношения (5) заметим, что

$$\Delta(fg) = \Delta f \cdot g + f \cdot \Delta g + \Delta f \cdot \Delta g.$$

Но однородная часть первой степени многочлена $\Delta f \cdot g$ равна $df \cdot g$, для многочлена $f \cdot \Delta g$ она равна $f \cdot dg$, а для многочлена $\Delta f \cdot \Delta g$ — нулю. Отсюда следует формула (5).

Следствие 1. *Отображение $f \to df$ является линейным отображением A-модуля $A[X_1, X_2, \ldots, X_p]$ в A-модуль однородных многочленов первой степени в кольце $B[Y_1, Y_2, \ldots, Y_p]$.*

Следствие 2. *Каждое из отображений $f \to D_i f$ является эндоморфизмом A-модуля $A[X_1, X_2, \ldots, X_p]$, для которого выполнено тождество*

$$D_i(fg) = D_i f \cdot g + f \cdot D_i g. \tag{6}$$

Следствие 3. *Для любого целого положительного n имеют место соотношения*

$$D_i(X_i^n) = nX_i^{(n-1)} \quad (1 \leqslant i \leqslant p), \tag{7}$$

$$D_j(X_i^n) = 0 \qquad (j \neq i). \tag{8}$$

Действительно, (7) вытекает из формулы (6) индукцией по n. С другой стороны, многочлен $\Delta(X_i^n)$ не содержит Y_j, откуда следует (8).

Предложение 2. *Пусть f — многочлен из кольца*

$$A[X_1, X_2, \ldots, X_p],$$

$u_i (1 \leqslant i \leqslant p)$ — p многочленов из кольца $A[Z_1, Z_2, \ldots, Z_q]$. Положим $h = f(u_1, u_2, \ldots, u_p)$, тогда

$$dh(Z_1, \ldots, Z_q;\ dZ_1, \ldots, dZ_q) = df(u_1, \ldots, u_p;\ du_1, \ldots, du_p). \tag{9}$$

Действительно, в силу определения

$$\Delta h = f(u_1 + \Delta u_1, \ldots, u_p + \Delta u_p) - f(u_1, \ldots, u_p).$$

Так как Δu_i — многочлены без свободного члена (по отношению к dZ_j), то однородная часть первой степени многочлена Δh такова же, как и у многочлена

$$df(u_1, \ldots, u_p;\ \Delta u_1, \ldots, \Delta u_p) = \sum_{i=1}^{p} D_i f(u_1, \ldots, u_p)\, \Delta u_i,$$

откуда следует формула (9).

Следствие. *В тех же обозначениях имеет место формула*

$$D_j h = \sum_{i=1}^{p} D_i f(u_1, u_2, \ldots, u_p)\, D_j u_i \quad (1 \leqslant j \leqslant q). \tag{10}$$

2. *Приложение: характеризация простых корней многочлена*

Предложение 3. *Для того чтобы корень $\alpha \in A$ многочлена $f \in A[X]$ был простым, необходимо и достаточно, чтобы α не являлся корнем многочлена Df.*

Действительно, в силу предположения $f = (X-\alpha)g$, где g — многочлен. При этом α является простым корнем в том и только в том случае, когда $g(\alpha) \neq 0$. По формуле (6) $Df = g + (X-\alpha)Dg$. Из этого вытекает, что $g(\alpha) = Df(\alpha)$, откуда следует предложение.

Более общо:

Предложение 4. *Если элемент $\alpha \in A$ является корнем порядка $k \geqslant 1$ многочлена $f \in A[X]$, то он является корнем порядка $\geqslant k-1$ многочлена Df. Если в кольце A из соотношения $k\xi = 0$ следует, что $\xi = 0$, то α является корнем порядка $k-1$ многочлена Df.*

Действительно, по предположению, $f = (X-\alpha)^k g$, где g уже не делится на $X-\alpha$. Из этого следует, что $Df = k(X-\alpha)^{k-1}g + (X-\alpha)^k Dg$. Это доказывает первую часть предложения. С другой стороны, из предыдущего соотношения вытекает, что если $(X-\alpha)^k$ делит Df, то $(X-\alpha)$ делит многочлен kg (поскольку $X-\alpha$ не является делителем нуля в кольце $A[X]$), т. е. (§ 2, предложение 5), что $kg(\alpha) = 0$. Если в кольце A из соотношения $k\xi = 0$ следует, что $\xi = 0$, мы получим, таким образом, что $g(\alpha) = 0$, а это противоречит предположению.

Если, напротив, в кольце A существует такой ненулевой элемент ξ, что $k\xi = 0$, то α может быть корнем произвольного порядка $\geqslant k-1$ многочлена Df. Например, пусть $k\xi = 0$ для всех $\xi \in A$; положим $g = (X-\alpha)^h + \beta$ с $\beta \neq 0$; тогда α является корнем порядка k многочлена f, но корнем порядка $\geqslant k+h-1$ многочлена Df.

Следствие. *Если элемент $\alpha \in A$ является корнем многочлена f и корнем порядка p многочлена Df, и если из соотношения $p!\,\xi = 0$ в кольце A следует, что $\xi = 0$, то порядок корня α многочлена f равен $p+1$.*

В самом деле, по предложению 4 α является корнем многочлена f, порядок кратности которого удовлетворяет неравенству

$1 \leqslant k \leqslant p+1$. Допустим, что $k < p+1$. Так как из $k\xi = 0$ следует, что $p!\,\xi = 0$, то в силу предположения $\xi = 0$. Таким образом, α будет корнем порядка $k-1$ многочлена Df, что противоречит предположению.

3. *Дифференцирования алгебры*

Следствие 2 предложения 1 приводит к обобщению понятия производной на случай произвольной алгебры:

Определение 3. *Пусть E — алгебра над коммутативным кольцом (с единицей) A. Назовем дифференцированием алгебры E любой эндоморфизм D A-модуля E, для которого $D(xy) = D(x)\,y + xD(y)$.*

Из этого определения индукцией по целым положительным p немедленно получается *формула Лейбница*

$$D^p(xy) = \sum_{k=0}^{p} \binom{p}{k} D^k(x)\, D^{p-k}(y) \qquad (11)$$

(используется соотношение между биномиальными коэффициентами $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$).

Примеры. 1) В алгебре многочленов $A[X_1, X_2, \ldots, X_n]$ n отображений D_i (n° 1) являются *дифференцированиями*, которые называют *n частными дифференцированиями* этой алгебры.

2. Для любого элемента $a \in E$ отображение $x \to ax - xa$ является дифференцированием в алгебре E, так как $a(xy) - (xy)\,a = (ax - xa)\,y + x(ay - ya)$. Такое дифференцирование называется *внутренним дифференцированием* алгебры E, задаваемым элементом a. Оно равно нулю только в том случае, когда элемент a принадлежит центру алгебры E.

Замечания. 1) Вместо $D(x)$ значение дифференцирования D на элементе $x \in E$ часто обозначается символом Dx.

2) Множество E может быть наделено несколькими структурами алгебры, которые все имеют одну и ту же структуру кольца. Если речь идет о дифференцировании *кольца* E, то необходимо уточнить, какая структура алгебры на E (имеющая в качестве структуры кольца структуру заданного кольца) рассматривается в этом случае. В частности, любое кольцо E можно рассматривать как алгебру над кольцом Z. Если говорят о дифференцировании кольца E, не уточняя его структуру как алгебры, то подразумевается, что речь идет о структуре алгебры над кольцом Z. Если E наделено структурой алгебры, структура кольца которой такова же, как и структура задан-

ного кольца, то любое дифференцирование этой алгебры является также и дифференцированием E, рассматриваемой как алгебра над кольцом Z.

Если E — алгебра с единицей e, то для любого дифференцирования D алгебры E имеем $D(e) = D(e^2) = D(e)\,e + eD(e) = 2D(e)$. Отсюда следует, что $D(e) = 0$. Из этого вытекает, что $D(ne) = nD(e) = 0$ для любого целого числа n и $D(\alpha e) = \alpha D(e) = 0$ для любого элемента $\alpha \in A$.

В частности, в кольце Z и в факторкольцах $Z/(n)$ всякое дифференцирование *нулевое*.

Если z — элемент из *центра* C алгебры E, то Dz *принадлежит* C для любого дифференцирования D алгебры E. Действительно, для любого $x \in E$ выполнено равенство $zx = xz$. Отсюда $D(zx) = D(xz)$, т. е. $Dz \cdot x + z \cdot Dx = Dx \cdot z + x \cdot Dz$. Ввиду того, что $z \cdot Dx = Dx \cdot z$, получаем $Dz \cdot x = x \cdot Dz$, что доказывает требуемое.

Пусть D_1 и D_2 — дифференцирования алгебры E. Немедленно проверяется, что операторы $D_1 - D_2$ и αD_1 (где α — произвольный элемент из A) также являются дифференцированиями алгебры E. Другими словами, множество дифференцирований алгебры E, которое мы будем обозначать символом $\mathfrak{D}(E)$, является подмодулем A-модуля $\mathfrak{L}(E)$ всех эндоморфизмов A-модуля E. Напротив, *произведение* $D_1D_2\,(= D_1 \circ D_2)$ дифференцирований D_1 и D_2 в кольце $\mathfrak{L}(E)$, вообще говоря, не является *дифференцированием*.

Например, в алгебре $E = A[X]$ выполнено равенство $D^2(X^2) = 2$. Но $D^2(X) = 0$ и, следовательно, $D^2(X)\,X + XD^2(X) = 0$. Это доказывает, что D^2 уже не является дифференцированием алгебры E, если характеристика алгебры E отлична от двух.

Предложение 5. *Пусть D_1 и D_2 — произвольные два дифференцирования алгебры E; тогда эндоморфизм $D = D_2D_1 - D_1D_2$ A-модуля E является дифференцированием алгебры E.*

Действительно, для любой пары элементов x, y из E имеет место тождество

$$\begin{aligned} D(xy) &= D_2(D_1(x)\,y + xD_1(y)) - D_1(D_2(x)\,y + xD_2(y)) = \\ &= D_2(D_1(x))\,y + D_1(x)\,D_2(y) + D_2(x)\,D_1(y) + \\ &+ xD_2(D_1(y)) - D_1(D_2(x))\,y - D_2(x)\,D_1(y) - \\ &- D_1(x)\,D_2(y) - xD_1(D_2(y)) = D(x)\,y + xD(y). \end{aligned}$$

Дифференцирование $D_2D_1 - D_1D_2$ обозначается обычно символом $[D_1, D_2]$.

Предложение 6. *Для любого дифференцирования D алгебры E и любого элемента a из центра алгебры E эндоморфизм $x \to aD(x)$ (обозначаемый aD) A-модуля E является дифференцированием алгебры E.*

Действительно, пусть x и y — произвольные элементы алгебры E; тогда $aD(xy) = aD(x)\,y + axD(y) = aD(x)\,y + x(aD(y))$ (в силу перестановочности элемента a со всеми элементами алгебры E).

Заметим, что, напротив, отображение $x \to D(ax)$ уже не является дифференцированием.

Следствие. *Множество $\mathfrak{D}(E)$ дифференцирований алгебры E, наделенное сложением и внешним законом композиции $(a, D) \to aD$, где a принадлежит центру C алгебры E, превращается в C-модуль.*

Из определения 3 тотчас вытекает, что для произвольного дифференцирования D алгебры E множество элементов $x \in E$, для которых $D(x) = 0$, является *подалгеброй* алгебры E (которую называют иногда подалгеброй *констант относительно* D). Из этого замечания вытекает следующее предложение:

Предложение 7. *Пусть S — система образующих алгебры E. Если значения двух дифференцирований D_1 и D_2 алгебры E одинаковы на всех элементах системы S, то эти дифференцирования совпадают.*

Действительно, оператор $D = D_1 - D_2$ является дифференцированием. Подалгебра алгебры E, образованная элементами x, для которых $D(x) = 0$, содержит S и, следовательно, совпадает с E.

Предложение 8. *Пусть E — алгебра $A[X_1, X_2, \ldots, X_n]$ многочленов от n переменных над кольцом A. Частные дифференцирования D_i $(1 \leqslant i \leqslant n)$ образуют базис E-модуля $\mathfrak{D}(E)$ дифференцирований алгебры E, причем $D_iD_j = D_jD_i$ для любых индексов i и j.*

Пусть D — произвольное дифференцирование алгебры E. Положим $D(X_i) = u_i$ для $1 \leqslant i \leqslant n$ (u_i — элементы алгебры $E = A \times$ $\times [X_1, X_2, \ldots, X_n]$). Ввиду предложения 6 оператор $D' = \sum_{i=1}^{n} u_iD_i$ является дифференцированием алгебры E, для которого $D'(X_i) = u_i (1 \leqslant i \leqslant n)$. Дифференцирования D и D' принимают одни и те же

значения на единичном элементе алгебры E и на каждом из X_i. Эти элементы порождают алгебру E. Таким образом (предложение 7), $D = D'$. С другой стороны, предположим, что v_i $(1 \leqslant i \leqslant n)$ — n элементов алгебры E, для которых $\sum_{i=1}^{n} v_i D_i = 0$ в $\mathscr{D}(E)$. Тогда, в частности, для любого индекса j справедливо равенство $\sum_{i=1}^{n} v_i D_i(X_j) = 0$, то есть $v_j = 0$. Таким образом, дифференцирования D_i образуют *базис* модуля $\mathscr{D}(E)$ относительно E. Наконец, отображения $D_{ij} = [D_i, D_j]$ являются дифференцированиями алгебры E (предложение 5), причем $D_{ij}(X_k) = 0$ для $1 \leqslant k \leqslant n$. Следовательно, (предложение 7) $D_{ij} = 0$, чем заканчивается доказательство.

Отметим, что два *произвольных* дифференцирования алгебры $A[X_1, X_2, \ldots, X_n]$, вообще говоря, не перестановочны друг с другом.

Предложение 9. *Пусть E — коммутативная алгебра с единицей над кольцом A, D — дифференцирование алгебры E.* Для любого семейства $(x_i)_{1 \leqslant i \leqslant n}$ *из n элементов алгебры E и любого многочлена $f \in A[X_1, X_2, \ldots, X_n]$ имеем*

$$D(f(x_1, x_2, \ldots, x_n)) = \sum_{i=1}^{n} D_i f(x_1, x_2, \ldots, x_n)\, Dx_i. \tag{12}$$

Действительно, для любого многочлена $f \in A[X_1, \ldots, X_n]$ положим

$$\varphi(f) = D(f(x_1, \ldots, x_n)) - \sum_{i=1}^{n} D_i f(x_1, \ldots, x_n)\, Dx_i.$$

Немедленно проверяется, что φ — линейное отображение A-модуля $A[X_1, X_2, \ldots, X_n]$ в A-модуль E и что

$$\varphi(fg) = \varphi(f)\, g(x_1, x_2, \ldots, x_n) + f(x_1, x_2, \ldots, x_n)\, \varphi(g).$$

Множество элементов $f \in A[X_1, X_2, \ldots, X_n]$, для которых $\varphi(f) = 0$, образует подалгебру алгебры $A[X_1, \ldots, X_n]$. Она содержит, очевидно, единицу и элементы X_i $(1 \leqslant i \leqslant n)$. Таким образом, эта подалгебра совпадает с алгеброй $A[X_1, X_2, \ldots, X_n]$, что доказывает предложение. (Можно было также установить этот факт непосредственно для любого одночлена, проведя индукцию по его степени.)

Отметим, что следствие предложения 2 является частным случаем предложения 9.

4. *Продолжение дифференцирования; производные рациональных дробей*

Предложение 10. *Пусть S — моноид, A — коммутативное кольцо с единицей, E — алгебра моноида S относительно кольца A. Для всякого дифференцирования D кольца A существует дифференцирование $\overline{D}$, притом единственное, кольца* (без операторов) *E, для которого $\overline{D}(as) = D(a)s$ при любом $a \in A$ и любом $s \in S$.*

Действительно, из сформулированного условия ясно, что если дифференцирование $\overline{D}$ существует, то $\overline{D}(z) = \sum_{s \in S} D(a_s) S$ для любого элемента $z = \sum_{s \in S} a_s S$ кольца E. Обратно, легко проверить, что отображение $\overline{D}$, определенное этой формулой, является дифференцированием алгебры E.

В частности, если E — алгебра многочленов $A[X_1, \ldots, X_n]$ над кольцом A, то для любого многочлена $f = \sum_{(n_i)} a_{n_1 n_2 \ldots n_p} X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p}$ обозначим символом f^D многочлен $\sum_{(n_i)} D(a_{n_1 n_2 \ldots n_p}) X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p}$. Из предложения 10 видно, что отображение $f \longrightarrow f^D$ является дифференцированием кольца E, которое *продолжает* заданное дифференцирование D кольца A. Говорят, что многочлен f^D получен *применением дифференцирования D к коэффициентам многочлена f.*

Предложение 11. *Пусть A — кольцо целостности, K — его поле дробей. Любое дифференцирование D кольца A можно одним и только одним способом продолжить до дифференцирования $\overline{D}$ поля K. Если u, v — два произвольных элемента кольца A, причем $v \neq 0$, то справедлива формула*

$$\overline{D}\left(\frac{u}{v}\right) = \frac{D(u)\,v - uD(v)}{v^2}. \tag{13}$$

Если существует дифференцирование $\overline{D}$ поля K, продолжающее дифференцирование D, то его единственность и формула (13) следуют немедленно. Действительно, пусть $w = \frac{u}{v}$ $(u \in A, v \in A, v \neq 0)$; тогда $u = vw$. Следовательно, $D(u) = D(v)\,w + v\overline{D}(w)$, откуда вытекает выражение (13) для $\overline{D}(w)$. Остается доказать существо-

вание $\overline{D}$. Для этого докажем, что из тождества $\frac{u}{v} = \frac{u_1}{v_1}$ (u, v, u_1, v_1 из A, $vv_1 \neq 0$) следует, что $\frac{\partial(u)v - uD(v)}{v^2} = \frac{D(u_1)v_1 - u_1D(v_1)}{v_1^2}$. Действительно, это соотношение записывается в виде $v(u_1vD \times (v_1) + v_1^2D(u)) = v_1(uv_1D(v) + v^2D(u_1))$. Пользуясь тем, что $uv_1 = u_1v$, получим $vv_1(uD(v_1) + v_1D(u)) = vv_1(u_1D(v) + vD(u_1))$. Это эквивалентно соотношению $uD(v_1) + v_1D(u) = u_1D(v) + vD(u_1)$, которое получается дифференцированием равенства $uv_1 = u_1v$. Таким образом, для любого элемента $w = \frac{u}{v}$ поля K можно определить элемент $\overline{D}(w)$ формулой (13) независимо от представления w в виде дроби. Немедленно проверяется, что $\overline{D}$ является дифференцированием, чем заканчивается доказательство.

Пусть K — произвольное поле. Каждое из дифференцирований D_i ($1 \leqslant i \leqslant n$) алгебры $K[X_1, X_2, \ldots, X_n]$ многочленов от n переменных над K можно в силу предложения 11 продолжить единственным способом до дифференцирования алгебры $E = K(X_1, X_2, \ldots, X_n)$ рациональных дробей от n переменных над K. Это дифференцирование называют также *частным дифференцированием по* X_i и обозначают символом D_i. Для произольной рациональной дроби f элемент D_if обозначается также символом $\frac{\partial f}{\partial X_i}$ или f'_{X_i} и называется *частной производной* многочлена f относительно X_i. Если два дифференцирования алгебры E совпадают на каждом многочлене, то они равны в силу формулы (13). Рассуждая, как в предложении 8, мы можем заключить из этого, что n частных дифференцирований D_i образуют *базис* векторного пространства $\mathscr{D}(E)$ (над полем E) дифференцирований алгебры E; при этом D_i перестановочны друг с другом.

Пусть F — коммутативная алгебра над полем K, f — рациональная дробь из поля $K(X_1, \ldots, X_n)$. Если семейство $(x_i)_{1 \leqslant i \leqslant n}$ элементов из F допускает подстановку (§ 3, n°2) в f, то в силу формулы (13) оно допускает подстановку и в каждую из частных производных D_if. Немедленно проверяется, что для любого дифференцирования D алгебры F формула (12) все еще имеет место.

Если исключена возможность путаницы, то часто пишут $\frac{\partial f}{\partial x_i}$ вместо $D_if(x_1, x_2, \ldots, x_n)$.

Замечание. Понятие дифференцирования алгебры E над коммутативным кольцом A можно обобщить следующим образом: пусть E — *подалгебра* алгебры F над A; назовем *дифференцированием E в F* любое линейное отображение D A-модуля E в A-модуль F, для которого $D(xy) = D(x)\,y + xD(y)$. Немедленно проверяется, что предложение 6 и его следствие, а также предложение 7 обобщаются на случай дифференцирований из E в F. Если предположить, что алгебра F *коммутативна*, то переносится и предложение 9. Предложение 11 остается справедливым, если предположить, что F — *поле*, *содержащее* кольцо целостности A. Наконец, предложение 10 распространяется также на случай, когда D — дифференцирование из A в некоторое коммутативное кольцо B, содержащее A и имеющее тот же единичный элемент. В этом случае $\overline{D}$ является дифференцированием алгебры E в алгебру F моноида S относительно кольца B.

Напротив, формула Лейбница (11) и предложение 5, вообще говоря, не имеют смысла для дифференцирования из алгебры E в алгебру F, ее содержащую. Кроме того, для дифференцирования D алгебры E в алгебру F образ Dz элемента z из центра алгебры E не обязательно принадлежит центру алгебры E.

Отметим, что *ограничение* любого дифференцирования алгебры F над кольцом A на подалгебру E является дифференцированием алгебры E в алгебру F.

5. *Дифференциальные формы*

Пусть E — *коммутативная* алгебра с единицей над кольцом A. Мы видели (предложение 6), что множество $\mathscr{D}(E)$ дифференцирований алгебры E наделено структурой *унитарного E-модуля*.

Определение 4. *Назовем дифференциальной формой на алгебре E любую линейную форму на E-модуле $\mathscr{D}(E)$ дифференцирований алгебры E.*

Таким образом, дифференциальные формы на E образуют E-модуль $\mathscr{D}(E)$ двойственный или сопряженный с $\mathscr{D}(E)$ в соответствии с общими обозначениями (гл. II, § 4); для любой дифференциальной формы ω и любого дифференцирования D

алгебры E будем применять символ $\langle D, \omega \rangle$ для значения ω на элементе D (основная билинейная форма). Если модуль $\mathscr{D}(E)$ имеет *базис* (D_i) из n элементов, то, как известно (loc. cit.), модуль $\mathscr{D}^*(E)$ имеет базис (ω_i) из n элементов, называемый *действительным базисом* к базису (D_i), для которого $\langle D_i, \omega_j \rangle = \delta_{ij}$ (символ Кронекера). Любое дифференцирование представляется тогда в виде $D = \sum_{i=1}^{n} \lambda_i D_i$, а любая дифференциальная форма — в виде $\omega = \sum_{i=1}^{n} \mu_i \omega_i$, причем $\langle D, \omega \rangle = \sum_{i=1}^{n} \lambda_i \mu_i$.

Пусть x — произвольный элемент алгебры E. Очевидно, отображение $D \to Dx$ модуля $\mathscr{D}(E)$ в A является *линейной формой*. Эта дифференциальная форма называется *полным дифференциалом* элемента x и обозначается символом dx. Другими словами, для любого элемента $x \in E$ и любого дифференцирования $D \in \mathscr{D}(E)$ имеет место равенство

$$\langle D, dx \rangle = Dx. \tag{14}$$

Отметим, что, вообще говоря, существуют дифференциальные формы, которые *не являются* полными дифференциалами элементов из E (см. упражнение 14).

Предложение 12. *Для любой пары элементов x, y алгебры E и любого элемента α кольца A имеют место равенства*

$$d(x+y) = dx + dy, \quad d(\alpha x) = \alpha\, dx, \quad d(xy) = x\, dy + y\, dx. \tag{15}$$

Докажем, например, третье из этих соотношений. Для любого дифференцирования D, в силу (14) и определения 3, справедлива цепочка равенств

$$\langle D, d(xy) \rangle = D(xy) = Dx \cdot y + x \cdot Dy = \\ = \langle D, y \cdot dx \rangle + \langle D, x \cdot dy \rangle = \langle D, y \cdot dx + x \cdot dy \rangle.$$

В силу определения дифференциальной формы это доказывает наше утверждение.

Для единичного элемента e алгебры E справедливо тождество $\langle D, de \rangle = De = 0$ для любого дифференцирования D. Таким образом, $de = 0$, следовательно, $d(\alpha e) = \alpha\, de = 0$ для любого $\alpha \in A$.

Если модуль $\mathscr{D}(E)$ имеет базис (D_i), а (ω_i) — соответствующий двойственный базис модуля $\mathscr{D}^*(E)$ дифференциальных

форм, то для любого элемента $x \in E$ верно тождество

$$dx = \sum_{i=1}^{n} D_i x \omega_i. \tag{16}$$

6. *Приложение к многочленам и рациональным дробям*

Рассмотрим, в частности, случай, когда E является алгеброй многочленов $A[X_1, X_2, \ldots, X_n]$. Формула (14) показывает при $X = X_j$ и $D = D_i$, что $\langle D_i, dX_j \rangle = D_i X_j = \delta_{ij}$. Таким образом, полные дифференциалы dX_i $(1 \leqslant i \leqslant n)$ образуют в модуле $\mathscr{D}^*(E)$ *двойственный базис* к базису (D_i), состоящему из n частных дифференцирований. Для любого многочлена $f \in E$ из формулы (16) вытекает следующее выражение для полного дифференциала:

$$df = \sum_{i=1}^{n} D_i f \, dX_i. \tag{17}$$

Это доказывает, что если отождествить E-модуль однородных многочленов первой степени в кольце $E[Y_1, Y_2, \ldots, Y_n]$ с E-модулем $\mathscr{D}^*(E)$, поставив в соответствие каждому элементу Y_i дифференциал dX_i, то полный дифференциал df *совпадет* с дифференциалом, определенным в n° 1 (этим оправдается совпадение использованных обозначений).

Пусть теперь E — поле $K(X_1, X_2, \ldots, X_n)$ рациональных дробей от n переменных над полем K. Дифференциалы dX_i по-прежнему образуют базис модуля $\mathscr{D}^*(E)$, двойственный к базису (D_i), а формула (17) применима к произвольной рациональной дроби f. Отметим, что если $f = u/v$, где u и v — два многочлена (или рациональные дроби), то $df = \dfrac{v\,du - u\,dv}{v^2}$.

Заметим, наконец, что для произвольной коммутативной алгебры E над кольцом A с единицей, для любого семейства $(x_i)_{1 \leqslant i \leqslant n}$ элементов алгебры E и для всякого многочлена f из кольца $A[X_1, X_2, \ldots, X_n]$ формулы (12) и (14) доказывают тождество

$$d(f(x_1, x_2, \ldots, x_n)) = \sum_{i=1}^{n} D_i f(x_1, \ldots, x_n)\, dx_i. \tag{18}$$

Эту формулу можно было бы также без труда вывести из формул (15). Тождество (18) справедливо и в том случае, когда E является алгеброй над полем K, f — рациональная дробь из поля $K(X_1, \ldots, X_n)$, а (x_i) — семейство элементов алгебры E, допускающее подстановку в дробь f.

Упражнения. 1) Доказать, что для любого однородного многочлена степени m в кольце $A[X_1, \ldots, X_n]$ справедливо «тождество Эйлера»:

$$\sum_{i=1}^{n} X_i \frac{\partial f}{\partial X_i} = mf(X_1, X_2, \ldots, X_n).$$

Обратно, доказать, что если в кольце A из соотношения $m!\,\xi=0$ следует, что $\xi=0$, то любой многочлен f, степень которого не превосходит m и который удовлетворяет предыдущему тождеству, является однородным многочленом степени m.

2) Доказать, что интерполяционную формулу Лагранжа (§ 2, n° 4) можно записать в виде

$$f(X) = \omega(X) \sum_{i=1}^{n} \frac{\beta_i}{\omega'(\alpha_i)(X-\alpha_i)},$$

где $\omega(X)=(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$. Вывести отсюда для любого многочлена $g \in K[X]$, степень которого не превосходит $n-2$, равенство

$$\sum_{i=1}^{n} \frac{g(\alpha_i)}{\omega'(\alpha_i)} = 0$$

(рассмотреть многочлен $f(X)=Xg(X)$).

3) Пусть $\alpha_i\ (1 \leqslant i \leqslant n)$ — n различных элементов поля K, $\beta_i\ (1 \leqslant i \leqslant n)$ и $\gamma_i\ (1 \leqslant i \leqslant n)$ — $2n$ произвольных элементов поля K. Доказать, что существует, и притом только один, многочлен $f \in K[X]$ степени $\leqslant 2n-1$, для которого $f(\alpha_i)=\beta_i$ и $f'(\alpha_i)=\gamma_i$ при $1 \leqslant i \leqslant n$ (интерполяционная формула Эрмита). (Начать с рассмотрения случая, когда $2n-1$ из $2n$ элементов β_i, γ_i равны нулю.)

4) Пусть K — поле характеристики нуль. Доказать, что всякая рациональная дробь $u \in K(X)$, для которой $Du=0$, равна константе.

5) Обобщить результаты упражнения 1 на случай однородных рациональных дробей (§ 3, упражнение 3) над полем характеристики нуль. (Рассмотреть рациональную дробь $\frac{1}{Z^m} f(ZX_1, ZX_2, \ldots, ZX_n)$ относительно Z и использовать результат упражнения 4.)

*6) а) Пусть A — коммутативное кольцо с единицей, в котором для любого ненулевого целого числа $n \in Z$ из соотношения $n\xi=0$

следует, что $\xi=0$. Доказать, что отображение $f \to f(\mathscr{D}_1, \ldots, \mathscr{D}_n)$ является изоморфизмом алгебры многочленов $A[X_1, \ldots, X_n]=E$ в алгебру (над A) эндоморфизмов A-модуля E (провести индукцию по n).

б) Пусть A—коммутативное кольцо с единицей характеристики $m>0$. Доказать, что $\mathscr{D}_i^m=0$ для любого частного дифференцирования $\mathscr{D}_i$ $(1 \leqslant i \leqslant n)$ в кольце $A[X_1, \ldots, X_n]$.

7) Пусть A—поле нулевой характеристики. Доказать, что для любого многочлена $f \in K[X_1, X_2, \ldots, X_n]$ справедливо равенство

$$f(X_1+Y_1, X_2+Y_2, \ldots, X_n+Y_n)= \\ =\sum_{p=0}^{\infty} \frac{1}{p!}(Y_1\mathscr{D}_1+Y_2\mathscr{D}_2+\ldots+Y_n\mathscr{D}_n)^p f$$

(«формула Тейлора для многочленов»). (Доказать сначала формулу для $n=1$, затем рассмотреть многочлен $f(X_1+ZY_1, \ldots, X_n+ZY_n)$.)

8) Пусть D_1, D_2, D_3—произвольные дифференцирования алгебры A. Доказать, что имеют место тождества $[\mathscr{D}_1, \mathscr{D}_1]=0$, $[\mathscr{D}_2, \mathscr{D}_1]+[\mathscr{D}_1, \mathscr{D}_2]=0$, $[[\mathscr{D}_1, \mathscr{D}_2], \mathscr{D}_3]+[[\mathscr{D}_2, \mathscr{D}_3], \mathscr{D}_1]+[[\mathscr{D}_3, \mathscr{D}_1], \mathscr{D}_2]=0$ («тождество Якоби», см. гл. I, § 5, упражнение 6).

9) Пусть A—алгебра над полем K нулевой характеристики, D—дифференцирование алгебры A, для которого $D^n=0$ при некотором целом положительном n. В алгебре $\mathscr{L}(A)$ эндоморфизмов векторного пространства A положим $u_t=\sum_{p=0}^{n-1} \frac{t^p}{p!}\mathscr{D}^p$ (при любом $t \in K$).

Доказать, что для любых двух элементов t и t' поля K справедливо соотношение $u_{t+t'}=u_t u_{t'}$. Вывести из этого, что отображения u_t являются автоморфизмами алгебры A, причем образуют абелеву группу, изоморфную факторгруппе аддитивной группы поля K.

*10) Пусть A—коммутативное кольцо с единицей, $E=M_n(A)$—алгебра квадратных матриц порядка n над кольцом A, $\mathscr{D}$—дифференцирование алгебры E, (E_{ij})—канонический базис (гл. II, § 6, n° 2) алгебры E над кольцом A. Доказать, что

$$\mathscr{D}(E_{ij})=(\beta_j-\beta_i)E_{ij}+\sum_{k \neq i} \alpha_{jk}E_{ik}-\sum_{k \neq j} \alpha_{ki}E_{kj},$$

где $(\beta_l)_{1 \leqslant i \leqslant n}$—некоторое семейство элементов кольца A, (α_{ij})—некоторое семейство элементов кольца A, определенное при $i \neq j$ (продифференцировать таблицу умножения элементов E_{ij}). Вывести отсюда, что любое дифференцирование $\mathscr{D}$ алгебры E является *внутренним* дифференцированием (n° 3).

11) Пусть E—алгебра, $\mathfrak{a}$—двусторонний идеал в алгебре E, $\mathscr{D}$—дифференцирование алгебры E, для которого $\mathscr{D}(\mathfrak{a}) \subset \mathfrak{a}$. Дока-

зать, что отображение $E/\mathfrak{a}$ в себя, полученное из $\mathscr{D}$ переходом к факторам, является дифференцированием алгебры $E/\mathfrak{a}$.

12) Пусть алгебра E является произведением конечного числа алгебр E_i над кольцом A ($1 \leqslant i \leqslant n$), для которых $E_i \cdot E_i = E_i$ (в частности, это всегда выполнено, если E обладает единичным элементом). Доказать, что для произвольного дифференцирования $\mathscr{D}$ алгебры E его ограничение $\mathscr{D}_i$ на E_i является дифференцированием алгебры E_i. Множество $\mathscr{D}(E)$ дифференцирований алгебры E, рассматриваемое как A-модуль, является прямой суммой A-модулей $\mathscr{D}(E_i)$. Так же верно, если алгебра E коммутативна, а $\mathscr{D}(E)$ рассматривается как E-модуль. Кроме того, каждый из модулей $\mathscr{D}(E_i)$ аннулируется всеми E_j с $j \neq i$.

13) Пусть E_1, E_2 — две алгебры над A, $\mathscr{D}_1$ — дифференцирование алгебры E_1, а $\mathscr{D}_2$ — дифференцирование алгебры E_2. Доказать, что существует дифференцирование D тензорного произведения $E = E_1 \otimes E_2$, для которого $D(x \otimes y) = (D_1 x) \otimes y + x \otimes (D_2 y)$ при любых $x \in E_1$ и $y \in E_2$.

*14) Пусть E — коммутативная алгебра с единицей над кольцом A. Обозначим символом $\mathscr{D}_p(E)$ p-ю внешнюю степень (гл. III, § 5, n° 5) E-модуля $\mathscr{D}(E)$ дифференцирований модуля E. Каждая линейная форма Ω на $\mathscr{D}_p(E)$, которую можно отождествить со знакопеременной полилинейной формой на $(\mathscr{D}(E))^p$ (loc. cit.), называется *внешней дифференциальной формой степени p* на алгебре E. Обозначим символом $\mathscr{D}_p^*(E)$ модуль, образованный этими формами.

а) Доказать, что для любой внешней дифференциальной формы $\Omega \in \mathscr{D}_p^*(E)$ отображение

$$(D_1, \ldots, D_{p+1}) \to \sum_{i=1}^{p+1} (-1)^{i+1} D_i(\langle \Omega, D_1 \wedge \ldots \wedge D_{i-1} \wedge D_{i+1} \ldots \wedge D_{p+1} \rangle) + \sum_{i<j} (-1)^{i+j+1} \langle \Omega, [D_i, D_j] \wedge D_1 \wedge \ldots \wedge D_{i-1} \wedge D_{i+1} \wedge \ldots \wedge D_{j-1} \wedge D_{j+1} \wedge \ldots \wedge D_{p+1} \rangle$$

является знакопеременной полилинейной формой на $(\mathscr{D}(E))^{p+1}$, или, что то же, линейной формой на $\mathscr{D}_{p+1}(E)$, которую обозначают символом $d\Omega$ (*внешний дифференциал* от Ω).

б) Доказать, что $d(d\Omega) = 0$ для любой внешней дифференциальной формы $\Omega \in \mathscr{D}_p^*(E)$ (использовать упражнение 8).

в) Предположим, что $\mathscr{D}(E)$ имеет конечный базис $(D_i)_{1 \leqslant i \leqslant n}$; пусть $(\omega_i)_{1 \leqslant i \leqslant n}$ — двойственный базис модуля $\mathscr{D}^*(E)$. Для любой конечной части H из p элементов интервала $[1, n]$ внешние дифференциальные формы степени p вида $\omega_H = \omega_{i_1} \wedge \omega_{i_2} \wedge \ldots \wedge \omega_{i_p}$ (где $(i_k)_{1 \leqslant k \leqslant p}$ — строго возрастающая последовательность элементов из H) образуют базис модуля $\mathscr{D}_p^*(E)$ (гл. III, § 8). Доказать, что для двух

дифференциальных форм Ω, Ω' степеней p и q соответственно выполнено равенство

$$d(\Omega \wedge \Omega') = (d\Omega) \wedge \Omega' + (-1)^p \Omega \wedge (d\Omega').$$

г) Предположим, что E — алгебра многочленов $A[X_1, \ldots, X_n]$ причем в кольце A уравнение $p!\,\xi = \eta$ имеет некоторое решение $\xi \in A$ для любого $\eta \in A$. Доказать, что внешняя дифференциальная форма Ω степени p имеет вид $d\omega$ в том случае, если $d\Omega = 0$ (провести индукцию по числу перемеяных).

§ 5. Формальные ряды

1. Определение формальных рядов

Пусть I — *конечное* множество индексов. Аддитивный моноид N^I удовлетворяет условию (D) главы II, § 7, n° 10, т. е. для каждого элемента (n_i) моноида N^I существует только конечное число пар $((p_i), (q_i))$ элементов из N^I таких, что $(p_i) + (q_i) = (n_i)$. Действительно, это равенство означает, что $p_i + q_i = n_i$ для любого $i \in I$, но для каждого $i \in I$ существует только $n_i + 1$ пара натуральных чисел (p_i, q_i), удовлетворяющих этому условию. Отсюда следует утверждение, так как множество I конечно.

Тем самым, мы можем рассматривать *расширенную алгебру* (гл. II, § 7, n° 10) моноида N^I относительно коммутативного кольца A с единицей. Эта алгебра коммутативна и содержит в качестве подалгебры (с той же единицей) алгебру *многочленов* (с коэффициентами из A) от переменных x_i $(i \in I)$, которая является *узкой* алгеброй моноида N^I над кольцом A.

Определение 1. *Для произвольного конечного множества индексов I расширенная алгебра моноида N^I над кольцом A* (коммутативным и обладающим единицей) *называется алгеброй формальных степенных рядов от переменных X_i $(i \in I)$ с коэффициентами в A и обозначается $A[[X_i]]_{i \in I}$. Всякий элемент этой алгебры называется формальным рядом от переменных X_i $(i \in I)$ с коэффициентами из A.*

Если I — конечная часть множества N, пишут $A[[X_{i_1}, \ldots, X_{i_p}]]$ вместо $A[[X_i]]_{i \in I}$, где $(i_k)_{1 \leqslant k \leqslant p}$ — последовательность элементов из I, расположенных в порядке возрастания.

Как принято для расширенных алгебр моноидов (гл. II, § 7, n° 10), формальный ряд $(\alpha_{(n_i)})_{(n_i)\in N^I}$ обозначается символом $\sum_{(n_i)} \alpha_{(n_i)} \prod_i X_i^{n_i}$ (подразумевается, что речь идет не о сумме многочленов в смысле главы I). Элементы $\alpha_{(n_i)} \prod_i X_i^{n_i}$ называются *членами* формального ряда, $\alpha_{(n_i)}$ — их *коэффициентами*. Многочлен от $X_i\,(i\in I)$ отождествляется с формальным рядом, имеющим только конечное число отличных от нуля коэффициентов.

Если I и I' — два конечных множества из p элементов, φ — взаимно однозначное отображение I на I', то линейное отображение алгебры $A[[X_i]]_{i\in I}$ в $A[[X_j]]_{j\in I'}$, которое каждому элементу $\sum \alpha_{(n_i)} \prod_i X_i^{n_i}$ первой из этих алгебр ставит в соответствие элемент $\sum \alpha_{(n_i)} \prod_i X_{\varphi(i)}^{n_i}$ второй алгебры, является изоморфизмом первой алгебры на вторую. В частности, алгебры формальных рядов, соответствующие всевозможным множествам индексов из p элементов, изоморфны; их называют *алгебрами формальных рядов от p переменных* с коэффициентами из A.

По определению главы II, § 7, n° 10 произведение двух формальных рядов алгебры $A[[X_1, X_2, \ldots, X_p]]$

$$u = \sum \alpha_{n_1 n_2 \ldots n_p} X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p},$$

$$v = \sum \beta_{n_1 n_2 \ldots n_p} X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p}$$

есть формальный ряд

$$w = \sum \gamma_{n_1 n_2 \ldots n_p} X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p},$$

где

$$\gamma_{n_1 n_2 \ldots n_p} = \sum \alpha_{h_1 h_2 \ldots h_p} \beta_{k_1 k_2 \ldots k_p}$$

и суммирование производится по таким парам $((h_i), (k_i))$, для которых $h_i + k_i = n_i$ при $1 \leqslant i \leqslant p$.

Пусть J — непустая часть множества I. Алгебру $A[[X_i]]_{i\in J}$ можно отождествить с подалгеброй алгебры $A[[X_i]]_{i\in I}$, состоящей из формальных рядов $\sum \alpha_{(n_i)} \prod_i X_i^{n_i}$, где $\alpha_{(n_i)} = 0$ для каждого элемента $(n_i)\in N^I$ такого, что $n_i \neq 0$ по крайней мере для одного индекса $i \in CJ$. Далее, пусть B — эта подалгебра, а K — (непустое)

дополнение к J в I. Определим *изоморфизм* кольца $A[[X_i]]_{i\in I}$, рассматриваемого как алгебра над B с алгеброй $B[[X_i]]_{i\in K}$ формальных рядов от переменных X_i с индексами $i\in K$ и коэффициентами из B следующим образом: формальному ряду $\sum \alpha_{(n_i)} \prod_{i\in I} X_i^{n_i}$ поставим в соответствие формальный ряд $\sum \beta_{(m_k)} \times \times \prod_{k\in K} X_k^{m_k}$, где

$$\beta_{(m_k)} = \sum \gamma_{(p_j)} \prod_{j\in J} X_j^{p_j}$$

и $\gamma_{(p_j)} = \alpha_{(n_i)}$, причем последовательность (n_i) определится условиями $n_i = p_i$ при $i\in J$, $n_i = m_i$ при $i\in K$. Наконец, пусть φ — некоторое представление кольца A в кольце B. Определим представление $\bar{\varphi}$ кольца $A[[X_i]]_{i\in I}$ в кольце $B[[X_i]]_{i\in I}$, которое продолжает φ, ставя в соответствие каждому формальному ряду $\sum \alpha_{(n_i)} \prod X_i^{n_i}$ формальный ряд $\sum \varphi(\alpha_{(n_i)}) \prod X_i^{n_i}$. Говорят, что этот последний ряд получается применением φ к коэффициентам формального ряда $\sum \alpha_{(n_i)} \prod X_i^{n_i}$.

В частности, пусть A' — подкольцо кольца A, обладающее той же единицей. Тогда тождественное отображение A' в A продолжается до тождественного отображения подкольца $A'[[X_i]]_{i\in I}$ в кольцо $A[[X_i]]_{i\in I}$. Ограничивая кольцо операторов алгебры $A[[X_i]]_{i\in I}$ кольцом A', эту алгебру можно рассматривать как алгебру над A'. Кольцо $A'[[X_i]]_{i\in I}$ тогда является *подалгеброй* алгебры $A[[X_i]]_{i\in I}$.

2. *Порядок формального ряда*

Пусть дан формальный ряд $u = \sum \alpha_{(n_i)} \prod_i X_i^{n_i}$. Назовем членами *полной степени* p ряда u те члены $\alpha_{(n_i)} \prod X_i^{n_i}$, для которых $\sum_{i\in I} n_i = p$. Сумма членов полной степени p ряда u является однородным *многочленом* u_p степени p, который еще называют *однородной частью степени* p формального ряда u (u_0 называют также *свободным членом* формального ряда u). Пусть u и v — два

формальных ряда, $w = uv$; тогда

$$w_p = \sum_{r=0}^{p} u_r v_{p-r}$$

для всех целых чисел $p \geqslant 0$.

Полным порядком (или просто *порядком*) произвольного формального ряда $u \neq 0$ называется наименьшее из чисел p такое, что однородная часть степени p формального ряда u не равна нулю. Пусть $\omega(u)$ — этот порядок. Для любой пары ненулевых формальных рядов u и v имеем

$$\omega(u+v) \geqslant \mathrm{Min}(\omega(u), \omega(v)) \quad \text{при} \quad u+v \neq 0, \tag{1}$$

$$\omega(uv) \geqslant \omega(u) + \omega(v) \quad \text{при} \quad uv \neq 0. \tag{2}$$

Кроме того, если $\omega(u) \neq \omega(v)$, то $u+v \neq 0$ и в (1) имеет место равенство.

Понятие порядка, в частности, применимо к *многочленам* от переменных X_i $(i \in I)$; его не следует смешивать со *степенью* многочлена (§ 1, n° 3). Порядок нуля *не определен*. Допуская вольность речи, иногда удобно говорить, что «формальный ряд f имеет порядок $\geqslant p$ (соответственно $> p$)», если однородная часть степени n формального ряда f равна нулю для всех $n < p$ (соответственно $n \leqslant p$). Таким образом, 0 оказывается «формальным рядом порядка $\geqslant p$» для любого $p \geqslant 0$ (см. § 1, n° 2).

Мы видели, что для непустой части J множества I, отличной от I, формальный ряд u из кольца $A[[X_i]]_{i \in K}$ можно рассматривать как формальный ряд от переменных X_i, $i \in J$, с коэффициентами в кольце $B = A[[X_i]]_{i \in K}$ (где $K = CJ$). Таким образом, введенным выше определениям соответствуют новые определения для формальных рядов $u \in A[[X_i]]_{i \in I}$. Член $a_{(n_i)} \prod_i X_i^{n_i}$ имеет *степень* p *относительно переменных* X_i, $i \in J$, если $\sum_{i \in J} n_i = p$. Сумма членов формального ряда u степени p относительно X_i, $i \in J$, является однородным многочленом степени p относительно этих переменных, называемым *однородной частью степени* p *относительно* X_i, $i \in J$, ряда u (или при $p = 0$ *свободным членом относительно переменных* X_i, $i \in J$). *Порядок* $\omega_J(u)$ формального ряда u относительно переменных X_i, $i \in J$, есть наименьшее из чисел $p \geqslant 0$, для которых однородная часть степени p ряда u относительно этих переменных не равна нулю. Неравенства (1) и (2) сохраняются при замене ω на ω_J.

3. Формальные ряды над областью целостности

Теорема 1. *Пусть A — область целостности (обладающая единицей). Тогда всякое кольцо формальных рядов $A[[X_i]]_{i\in I}$ над кольцом A является областью целостности.*

Действительно, пусть u и v — формальные ряды, отличные от нуля; тогда однородная часть f (соответственно g) ряда u (соответственно v) степени $\omega(u)$ (соответственно $\omega(v)$) представляет собой ненулевой многочлен. Однородной частью степени $\omega(u)+\omega(v)$ формального ряда uv будет многочлен fg, который не равен нулю (§ 1, теорема 1). Следовательно, $uv\neq 0$.

Следствие. *Пусть A — область целостности, u и v — два ненулевых формальных ряда из кольца $A[[X_i]]_{i\in I}$; тогда*

$$\omega(uv)=\omega(u)+\omega(v). \tag{3}$$

Отсюда немедленно следует подобное же равенство для любой непустой части J множества I:

$$\omega_J(uv)=\omega_J(u)+\omega_J(v). \tag{4}$$

4. Бесконечные суммы формальных рядов

Пусть A — коммутативное кольцо с единицей, L — некоторое множество индексов, $(u_\lambda)_{\lambda\in L}$ — семейство формальных рядов кольца $A[[X_i]]_{i\in I}$. Предположим, что порядок $\omega(u_\lambda)$ *стремится к* $+\infty$ *по фильтру дополнений к конечным частям множества* L, то есть (Общ. топол. гл. IV, § 4) для любого целого числа m существует такая конечная часть J множества L, что при всех $\lambda\notin J$ либо $u_\lambda=0$, либо $\omega(u_\lambda)\geqslant m$. В этих условиях для каждого $(n_i)\in\mathbf{N}^I$ существует только *конечное* число индексов λ, для которых коэффициенты при $\prod_i X_i^{n_i}$ в u_λ не равны нулю, так как это возможно лишь в случае $\omega(u_\lambda)\leqslant\sum_i n_i$. Таким образом, можно определить формальный ряд s, коэффициент при $\prod_i X_i^{n_i}$ в котором для любого (n_i) равен сумме коэффициентов при $\prod_i X_i^{n_i}$ в формальных рядах u_λ (это — сумма конечного числа ненулевых членов). Говорят, что семейство (u_λ) *суммируемо* и что формальный ряд s является суммой *этого* семейства, и пишут $s=\sum_{\lambda\in L}u_\lambda$. В случае, когда

L — некоторая часть множества N, пишут также $s = u_{k_1} + u_{k_2} + \ldots + u_{k_n} + \ldots$, где (k_n) — последовательность элементов множества L, расположенная в порядке возрастания. Из определения следует, что при $s \neq 0$

$$\omega\left(\sum_{\lambda \in L} u_\lambda\right) \geqslant \operatorname*{Min}_{\lambda \in L} \omega(u_\lambda). \tag{5}$$

Это определение оправдывает запись формального ряда в виде $\sum_{(n_i)} a_{(n_i)} \prod_i X_i^{n_i}$. Действительно, этот ряд, в силу сказанного, является суммой счетного семейства многочленов $a_{n_i} \prod_i X_i^{n_i}$ (здесь множество индексов L совпадает с $\boldsymbol{N}^I$). Подобным же образом семейство $u_n (n \in \boldsymbol{N})$, где u_n — однородная часть степени n формального ряда u, суммируемо и $u = u_0 + u_1 + \ldots + u_n + \ldots$

Предложение 1. *Пусть L — некоторое множество индексов, $(u_\lambda)_{\lambda \in L}$ — суммируемое семейство формальных рядов кольца $A[[X_i]]_{i \in I}$. Для любого разбиения $(L_\mu)_{\mu \in M}$ множества L каждое из подсемейств $(u_\lambda)_{\lambda \in L_\mu}$ суммируемо. Если S_μ — сумма этого семейства, то семейство формальных рядов $(S_\mu)_{\mu \in M}$ суммируемо и имеет ту же сумму, что и семейство $(u_\lambda)_{\lambda \in L}$.*

Первая часть предложения является непосредственным следствием определения суммируемого семейства. Далее, для каждого $(n_i) \in \boldsymbol{N}^I$ пусть H — конечная часть множества L, состоящая из тех λ, для которых коэффициент при $\prod_i X_i^{n_i}$ в u_λ не равен нулю, и пусть J — конечная часть множества M, состоящая из таких индексов μ, что L_μ содержит по крайней мере один элемент из H. Очевидно, что коэффициент при $\prod_i X_i^{n_i}$ в S_μ равен нулю для $\mu \notin J$, а коэффициент при $\prod_i X_i^{n_i}$ в $\sum_{\lambda \in L} u_\lambda$ тот же, что в $\sum_{\mu \in J} S_\mu$, откуда и следует предложение.

Предложение 2. *Пусть $(u_\lambda)_{\lambda \in L}$ и $(v_\mu)_{\mu \in M}$ — два суммируемых семейства формальных рядов кольца $A[[X_i]]_{i \in I}$. Тогда семейство $(u_\lambda v_\mu)_{(\lambda, \mu) \in L \times M}$ суммируемо и*

$$\sum_{(\lambda, \mu) \in L \times M} u_\lambda v_\mu = \left(\sum_{\lambda \in L} u_\lambda\right)\left(\sum_{\mu \in M} v_\mu\right). \tag{6}$$

Действительно, для любого целого числа m существует конечная часть H множества L и конечная часть J множества M такие, что для любого $\lambda \notin H$ и любого $\mu \notin J$ справедливы неравенства $\omega(u_\lambda) \geqslant m$ и $\omega(v_\mu) > m$. Из неравенства (2) следует, что $\omega(u_\lambda v_\mu) \geqslant m$ для каждого $(\lambda, \mu) \notin H \times J$. Применяя предложение 1, получим

$$\sum_{(\lambda,\mu)\in L\times M} u_\lambda v_\mu = \sum_{\lambda\in L}\Big(\sum_{\mu\in M} u_\lambda v_\mu\Big) = \sum_{\lambda\in L} u_\lambda\Big(\sum_{\mu\in M} v_\mu\Big) = \Big(\sum_{\lambda\in L} u_\lambda\Big)\Big(\sum_{\mu\in M} v_\mu\Big).$$

5. *Подстановка формальных рядов в формальный ряд*

Определения § 2 n° 1, в частности, позволяют определить выражение $f(u_1, u_2, \ldots, u_p)$, где f — *многочлен* кольца $A[X_1, \ldots, X_p]$, а $u_i (1 \leqslant i \leqslant p)$ — формальные ряды, принадлежащие кольцу $A[[Y_1, Y_2, \ldots, Y_q]]$. $f(u_1, u_2, \ldots, u_p)$ — снова формальный ряд, принадлежащий тому же кольцу. Мы увидим, что это определение можно распространить на случай, когда f — *формальный ряд*, принадлежащий кольцу $A[[X_1, X_2, \ldots, X_p]]$, наложив некоторые ограничения на формальные ряды u_i.

Итак, пусть $f = \sum_{(n_i)} a_{(n_i)} \prod_i X_i^{n_i}$ — формальный ряд от p переменных X_i $(1 \leqslant i \leqslant p)$. Предположим, что p рядов $u_i (1 \leqslant i \leqslant p)$ имеют *строго положительный порядок* (или, как еще говорят, *не содержит свободных членов*). По формуле (2) порядок ряда $u_1^{n_1} u_2^{n_2} \ldots u_p^{n_p}$ не менее чем $n_1 + n_2 + \ldots + n_p$. Следовательно, семейство $(a_{n_1 n_2 \ldots n_p} u_1^{n_1} \ldots u_p^{n_p})_{(n_i)\in N^I}$ *суммируемо*. По определению его *сумма* обозначается символом $f(u_1, u_2, \ldots, u_p)$. Говорят, что этот формальный ряд получается *подстановкой в ряд f рядов u_i от переменных X_i* $(1 \leqslant i \leqslant p)$.

Заметим, что это определение позволяет, в частности, пользоваться записью $f = f(X_1, X_2, \ldots, X_p)$.

Предложение 3. *Пусть u_i $(1 \leqslant i \leqslant p)$ — p формальных рядов без свободных членов, принадлежащих кольцу $A[[Y_1, Y_2, \ldots, Y_q]]$. Отображение $f \to f(u_1, u_2, \ldots, u_p)$ алгебры $A[[X_1, X_2, \ldots, X_p]]$ в алгебру $A[[Y_1, Y_2, \ldots, Y_q]]$ является представлением.*

Все сводится к доказательству того, что если f и g — два формальных ряда от переменных X_i и $h=fg$, то

$$h(u_1, u_2, \ldots, u_p)=f(u_1, u_2, \ldots, u_p)\,g(u_1, u_2, \ldots, u_p).$$

Это вытекает из предложений 1 и 2 и определения произведения двух формальных рядов.

6. *Обратимые формальные ряды*

Предложение 4. *Для того чтобы формальный ряд и кольца* $A[[X_1, X_2, \ldots, X_p]]$ *был обратим в этом кольце, необходимо и достаточно, чтобы его свободный член был обратим в кольце* A.

Условие необходимо, так как если v — формальный ряд кольца $A[[X_1, X_2, \ldots, X_p]]$ и $uv=1$, то для свободных членов α_0 и β_0 рядов u и v выполняется соотношение $\alpha_0\beta_0=1$. Обратно, пусть u — формальный ряд с обратимым свободным членом, тогда $u=\alpha_0-v=\alpha_0(1-\alpha_0^{-1}v)$, где v — ряд без свободного члена. Учитывая предложение 3, получаем предложение 4 как следствие следующего результата, проверка которого проводится непосредственно.

Предложение 5. *В кольце* $A[[T]]$ *формальных рядов от одного переменного многочлен* $1-T$ *обратим и*

$$(1-T)^{-1}=\sum_{n=0}^{\infty} T^n. \tag{7}$$

В обозначениях предложения 4 элемент, обратный к u, совпадает, тем самым, с формальным рядом $\Sigma\alpha_0^{-(n+1)}v^n$.

В частности, из предложения 4 вытекает, что *многочлен и кольца* $A[X_1, X_2, \ldots, X_p]$, имеющий обратимый в A свободный член, обратим в кольце степенных рядов $A[[X_1, X_2, \ldots, X_p]]$.

Пусть K — поле. В поле $K(X_1, X_2, \ldots, X_p)$ рациональных дробей от p переменных над K рассмотрим множество рациональных дробей $\frac{u}{v}$, у которых u — произвольный многочлен, а v — многочлен с ненулевым свободным членом. Ясно, что это множество является *подкольцом* (но не подполем) поля $K(X_1, X_2, \ldots, X_p)$ и что отображение $\frac{u}{v} \longrightarrow uv^{-1}$ определяет

изоморфизм этого кольца в кольцо формальных рядов $K[[X_1, X_2, \ldots, X_p]]$. Формальный ряд uv^{-1} называют *разложением* рациональной дроби $\frac{u}{v}$ и чаще всего отождествляют с этой дробью.

7. *Поле дробей кольца формальных рядов от одной переменной над полем*

Пусть K — поле; обозначим символом $K((X_1, X_2, \ldots, X_p))$ *поле дробей* области целостности $K[[X_1, X_2, \ldots, X_p]]$. Мы увидим, что элементы поля дробей $K((X))$ кольца формальных рядов от *одной* переменной над K могут быть представлены в особенно простой форме. Всякий формальный ряд $u \neq 0$ порядка h в кольце $K[[X]]$ однозначно записывается в виде $u = X^h v$, где v — формальный ряд порядка 0, и, следовательно (предложение 4), обратимый в кольце $K[[X]]$. Пусть X^{-1} — элемент поля $K((X))$, обратный к элементу $X \neq 0$. Положим, как обычно, $X^{-h} = (X^{-1})^h = (X^h)^{-1}$ для всех натуральных $h \geqslant 0$.

Мы покажем, что всякий ненулевой элемент поля дробей $K((X))$ может быть записан *единственным образом* в виде $X^h w$, где w — формальный ряд порядка 0, а K — целое число (положительное или отрицательное). Действительно, частное $(X^m u)/(X^n v)$ двух формальных рядов кольца $K[[X]]$ ($m \geqslant 0$, $n \geqslant 0$, u, v — ряды порядка 0) записывается в виде $X^{m-n} u v^{-1}$. С другой стороны, если $X^r w_1 = X^s w_2$, где w_1 и w_2 имеют нулевой порядок, то $r = s$, так как, если, например, $r > s$, то $X^{r-s} = w_2 w_1^{-1}$, и правая часть равенства имеет порядок 0, что невозможно. Произвольный элемент u кольца $K((X))$, представимый в виде $u = X^h w = X^h(\alpha_0 + \alpha_1 X + \ldots)$, $\alpha_0 \neq 0$, записывают также в виде $u = \alpha_0 X^h + \alpha_1 X^{h+1} + \ldots + \alpha_n X^{h+n} + \ldots$ Элементы кольца $K((X))$ называют *обобщенными формальными рядами* относительно X или просто *формальными рядами*, если это не может привести к недоразумению (в этом случае элементы кольца $K[[X]]$ называют *формальными рядами с положительными степенями*). Целое число k (которое, если оно неотрицательно, является порядком ряда u) тоже называется *порядком* обобщенного формального ряда u. Непосредственно проверяется, что отношения (1) и (3) остаются верными для обобщенных формальных рядов. В частности, если $u \neq 0$, то $\omega(u^{-1}) = -\omega(u)$.

Кольцо $K[X]$ многочленов от X является подкольцом кольца $K[[X]]$. Поэтому *всякая* рациональная дробь $\frac{u}{v}$ (u и v — многочлены, $v \neq 0$) может быть отождествлена с (обобщенным) формальным рядом uv^{-1} поля $K((X))$, который называется ее *разложением*. Таким образом, поле $K(X)$ рациональных дробей от одной переменной отождествляется с подполем поля $K((X))$.

Эти результаты *не распространяются* на поля дробей формальных рядов более одной переменной: не для всякого формального ряда u кольца $K[[X_1, X_2, \ldots, X_p]]$ существует формальный ряд $v \in K[[X_1, X_2, \ldots, X_p]]$ и целое число m такие, что

$$(X_1 X_2 \ldots X_p)^{-m} uv = 1$$

(см. упражнение 7).

8. *Дифференцирования в алгебре формальных рядов*

Предложение 6. *Пусть A — коммутативное кольцо с единицей, B — его подкольцо, обладающее той же единицей, что и A. Всякое дифференцирование D кольца многочленов $A[X_1, X_2, \ldots, X_p]$ (рассматриваемого как алгебра над B) со значениями в кольце формальных рядов $A[[X_1, X_2, \ldots, X_p]]$ однозначно продолжается до дифференцирования $\overline{D}$ кольца $A[[X_1, X_2, \ldots, X_p]]$ (рассматриваемого как алгебра над B).*

Действительно, для левого $(n_i) \in \mathbf{N}^I$ можно написать равенство

$$D\left(\prod_i X_i^{n_i}\right) = \sum_{i=1}^{p} n_i X_1^{n_1} \ldots X_{i-1}^{n_{i-1}} X_i^{n_i - 1} X_{i+1}^{n_{i+1}} \ldots X_p^{n_p} DX_i,$$

из которого непосредственно вытекает следующая лемма.

Лемма. *Для любого многочлена $u \in A[X_1, X_2, \ldots, X_p]$ имеет место неравенство $\omega(Du) \geqslant \omega(u) - 1$, если $Du \neq 0$.*

Пусть теперь $u = \sum_{n=0}^{\infty} u_n$ — формальный ряд кольца $A[[X_1, X_2, \ldots, X_p]]$, где u_n — однородные части степени n ряда u. Если $Du_n \neq 0$, то по лемме $\omega(Du_n) \geqslant n-1$. Следовательно, семейство $(Du_n)_{n \in \mathbf{N}}$ суммируемо. Покажем, что отображение $\overline{D}$, определенное формулой $\overline{D}u = \sum_{n=0}^{\infty} Du_n$, представляет собой дифференцирование кольца $A[[X_1, X_2, \ldots, X_p]]$, которое продолжает D.

Достаточно доказать, что $\overline{D}(uv) = \overline{D}u \cdot v + u \cdot \overline{D}v$ для любых двух формальных рядов u и v, а это непосредственно вытекает из предложения 2 и выражения однородной части степени n ряда uv через однородные части степеней $\leqslant n$ рядов u и v.

Остается доказать, что $\overline{D}$ — единственное дифференцирование кольца $A[[X_1, X_2, \ldots, X_p]]$, которое продолжает D. Для этого достаточно установить, что дифференцирование D_0 алгебры $A[[X_1, X_2, \ldots, X_p]]$, отображающее в нуль любой многочлен, тождественно равно нулю. Итак, пусть u — произвольный формальный ряд, w_r — многочлен, являющийся суммой однородных частей ряда u степени $\leqslant r$. Формальный ряд $u - w_r$ можно записать в виде $\sum v_{n_1 \ldots n_p} X_1^{n_1} \ldots X_p^{n_p}$, где (n_i) пробегает *конечное* подмножество множества $\mathbf{N}^I$, состоящее из элементов, для которых $\sum_{i=1}^{p} n_i = r$, а $v_{n_1 n_2 \ldots n_p}$ — формальные ряды. По лемме $D_0(u - w_r)$ равно нулю или имеет порядок, не меньший $r - 1$. С другой стороны, по предположению, $D_0(u) = D_0(u - w_r)$. Если $D_0 u \neq 0$, то порядок ряда $D_0 u$ должен быть не меньше $r - 1$ для любого целого числа r, что невозможно.

В частности, каждое *частное дифференцирование* D_i $(1 \leqslant i \leqslant p)$ кольца $A[X_1, X_2, \ldots, X_p]$ продолжается до дифференцирования кольца $A[[X_1, X_2, \ldots, X_p]]$, которое мы будем обозначать одним из символов D_i или $\frac{\partial}{\partial X_i}$. Таким образом,

$$D_i\left(\sum a_{n_1 n_2 \ldots n_p} X_1^{n_1} \ldots X_p^{n_p}\right) = \sum n_i a_{n_1 n_2 \ldots n_p} X_1^{n_1} \ldots X_i^{n_i - 1} \ldots X_p^{n_p}.$$

Из предложения 6 этого параграфа и предложения 8 § 4 следует, что $D_i D_j = D_j D_i$ для любых i и j.

Предложение 7. *Частные дифференцирования* D_i $(1 \leqslant i \leqslant p)$ *образуют базис E-модуля $\mathscr{D}(E)$ дифференцирований кольца E, рассматриваемого как алгебра над кольцом A.*

Действительно, пусть D — произвольное дифференцирование алгебры E, $D(X_i) = u_i$ $(u_i \in E)$. Тогда $D - \Sigma u_i D_i$ — тоже дифференцирование кольца E, которое, по предположению, равно нулю для элементов кольца A и всех X_i. Следовательно (§ 4, предложение 7), оно равно нулю для всех многочленов и, наконец (предложение 6), для всех элементов кольца E.

Из этого предложения следует, что p дифференциалов dX_i $(1 \leqslant i \leqslant p)$ образуют *базис* (дуальный к базису (D_i)) модуля $\mathscr{D}(E)$ *дифференциальных форм* на E (§ 4, n° 5). Таким образом, полный дифференциал произвольного формального ряда u задается формулой

$$du = \sum_{i=1}^{p} D_i u \, dX_i = \sum_{i=1}^{p} \frac{\partial u}{\partial X_i} \, dX_i. \tag{8}$$

Формальный ряд $u(X_1+Y_1, X_2+Y_2, \ldots, X_p+Y_p)$, являющийся вполне определенным элементом кольца $A[[X_1 \ldots X_p, Y_1 \ldots Y_p]]$ (n° 5), можно также рассматривать как элемент кольца формальных рядов $E[[Y_1, Y_2, \ldots, Y_p]]$ (n° 1). Легко проверяется, что многочлен $\sum_{i=1}^{p} D_i u Y_i$ является *однородной частью первой степени относительно* Y_i ряда $u(X_1+Y_1, \ldots, X_p+Y_p)$ или, что сводится к тому же, ряда

$$\Delta u = u(X_1+Y_1, \ldots, X_p+Y_p) - u(X_1, \ldots, X_p).$$

Ввиду этого результата и формулы (8) многочлен $\Sigma D_i u Y_i$ относительно Y_i часто обозначается символом

$$du(X_1, \ldots, X_p; \quad Y_1, \ldots, Y_p).$$

Предложение 8. *Пусть f — формальный ряд кольца $A[[X_1, X_2, \ldots, X_p]]$, u_i $(1 \leqslant i \leqslant p)$ — p формальных рядов без свободных членов кольца $A[[Z_1, Z_2, \ldots, Z_q]]$. Положим $h = f(u_1, u_2, \ldots, u_p)$; тогда*

$$dh = \sum_{i=1}^{p} D_i f(u_1, u_2, \ldots, u_p) \, du_i. \tag{9}$$

Действительно, положим $\Delta u_i = u_i(Z_1+T_1, \ldots, Z_q+T_q) - u_i(Z_1, \ldots, Z_q)$; тогда однородная часть первой степени формального ряда (относительно T_j) $\Delta h = f(u_1+\Delta u_1, \ldots, u_p+\Delta u_p) - f(u_1, \ldots, u_p)$ совпадает с однородной частью первой степени ряда $df(u_1 \ldots u_p; \Delta u_1, \ldots, \Delta u_p)$, так как ряды Δu_i не имеют свободных членов. Отсюда тотчас следует предложение.

Предложение 9. *Пусть u — формальный ряд кольца $A[[X_1, \ldots, X_p]]$. Положим*

$$u(X_1+Y_1, \ldots, X_p+Y_p) = \sum g_{n_1 n_2 \ldots n_p}(X_1, \ldots, X_p) Y_1^{n_1} Y_2^{n_2} \ldots Y_p^{n_p};$$

тогда

$$\left(\frac{\partial}{\partial X_1}\right)^{n_1}\left(\frac{\partial}{\partial X_2}\right)^{n_2}\dots\left(\frac{\partial}{\partial X_p}\right)^{n_p}u(X_1,\ X_2,\ \dots,\ X_p)=$$
$$=n_1!n_2!\dots!n_p!g_{n_1\dots n_p}(X_1,\ \dots,\ X_p) \quad (10)$$

(«формула Тейлора»).

Действительно, из определений непосредственно следует, что свободный член формального ряда относительно Y_i

$$\left(\frac{\partial}{\partial Y_1}\right)^{n_1}\left(\frac{\partial}{\partial Y_2}\right)^{n_2}\dots\left(\frac{\partial}{\partial Y_p}\right)^{n_p}u(X_1+Y_1,\ \dots,\ X_p+Y_p) \quad (11)$$

есть $n_1!n_2!\dots!n_p!g_{n_1n_2\dots n_p}(X_1,\ X_2,\ \dots,\ X_p)$. Из предложения 8 вытекает, что ряд (11) получается подстановкой X_i+Y_i вместо X_i $(1\leqslant i\leqslant n)$ в формальный ряд

$$\left(\frac{\partial}{\partial X_1}\right)^{n_1}\left(\frac{\partial}{\partial X_2}\right)^{n_2}\dots\left(\frac{\partial}{\partial X_p}\right)^{n_p}u(X_1,\ X_2,\ \dots,\ X_p).$$

Предложение доказано.

9. *Разрешимость уравнений в кольце формальных рядов*

Предложение 10. *Пусть* $f_i(Y_1, Y_2, \dots, Y_q, X_1, X_2, \dots, X_p)$ $(1\leqslant i\leqslant q)$ — *q формальных рядов без свободных членов кольца* $A[[Y_1, Y_2, \dots, Y_q, X_1, X_2, \dots, X_p]]$. *Если свободный член относительно всех* Y_i *формального ряда* $\Delta=\det\left(\frac{\partial f_i}{\partial Y_j}\right)$ *обратим в кольце* $A[[X_1, X_2, \dots, X_p]]$, *то в этом кольце существует единственная система q формальных рядов без свободных членов* $u_i(X_1, \dots, X_p)$ *такая, что*

$$f_i(u_1,\ u_2,\ \dots,\ u_q,\ \ X_1,\ X_2,\ \dots,\ X_p)=0$$

для $1\leqslant i\leqslant q$.

Действительно, пусть

$$f_i=f_{i0}+\sum_{j=1}^{q}f_{ij}Y_j+\sum_{(n_j)}f_{i;\,n_1\dots n_q}Y_1^{n_1}\dots Y_q^{n_q} \quad (1\leqslant i\leqslant q), \quad (12)$$

где во второй сумме все члены имеют степень больше единицы относительно Y_j; f_{i0}, f_{ij} и $f_{in_1\dots n_q}$ — элементы кольца $E=A[[X_1, X_2, \dots, X_p]]$, причем f_{i0} не имеют свободных членов. По пред-

положению, матрица $F=(f_{ij})$ обратима (гл. III, § 6, теорема 2); пусть $G=(g_{ij})$ — ее обратная. Пусть $g_i=\sum_{j=1}^{q} g_{ij}f_j$; тогда

$$g_i=-h_{i0}+Y_i-\sum_{(n_j)} h_{i;\,n_1\ldots n_q}Y_1^{n_1}\ldots Y_q^{n_q} \quad (1\leqslant i\leqslant q),$$

где h_{i0} и $h_{i;\,n_1\ldots n_q}$ — элементы кольца E, и h_{i0} не содержат свободных членов. Так как $f_i=\sum_{j=1}^{q} f_{ij}g_j$, достаточно доказать предложение для рядов g_i. Предположим, что задача решена, тогда

$$u_i=h_{i0}+\sum_{(n_j)} h_{i;\,n_1\ldots n_q}u_1^{n_1}\ldots u_q^{n_q} \quad (1\leqslant i\leqslant q). \tag{13}$$

Пусть u_{im} — однородная часть степени m ряда u_i и $v_{im}=\sum_{k=1}^{m} u_{ik}$ — сумма тех членов ряда u_i, полная степень которых не превосходит m. В формальном ряду $h_{i;\,u_1\ldots u_q}u_1^{n_1}\ldots u_q^{n_q}$, где $\sum_{j=1}^{q} n_j\geqslant 2$, однородная часть степени m та же, что в ряду $h_{i;\,n_1\ldots n_q}v_{1,m-1}^{n_1}\ldots v_{q,m-1}^{n_q}$, так как u_i — ряды без свободного члена. Из равенства (13) вытекает, что $u_{i1}=v_{i1}$ совпадает с однородной частью первой степени ряда h_{i0} и что для любого $m>1$ u_{im} определяется рекуррентно, как однородная часть степени m ряда

$$h_{i0}+\sum h_{i;\,n_1\ldots n_q}v_{1,m-1}^{n_1}\ldots v_{q,m-1}^{n_q}.$$

Этим одновременно доказывается существование и единственность рядов u_i, так как ясно, что если ряды u_{im} определяются рекуррентно указанным выше способом, то ряды $u_i=\Sigma u_{im}$ удовлетворяют системе (13).

10. *Топологические интерпретации*

Большую часть результатов этого параграфа удобно формулировать в топологических терминах, которые подсказывают возможность дальнейших обобщений. Рассмотрим кольцо формальных рядов $E=A[[X_1, X_2, \ldots, X_p]]$ и для каждого числа $n\geqslant 0$ символом $\mathfrak{a}_n$ обозначим множество рядов $u\in E$ порядка, не меньшего n. Неравенства (1) и (2) показывают, что $\mathfrak{a}_n$ — *идеал* кольца

E. Так как $\mathfrak{a}_n \subset \mathfrak{a}_m$ при $m \leqslant n$, эти идеалы образуют базис некоторого фильтра, и их пересечение равно нулю. Следовательно, они образуют *фундаментальную систему окрестностей нуля* в некоторой топологии кольца E, которая согласована со структурой аддитивной группы E (Общ. топол., гл. III, § 1, n° 2), а также, что легко проверяется, со структурой *кольца* E (аксиомы (AV_1) и (AV_{11}) из Общ. топол., гл. III, § 5, n° 1 проверяются тривиально). Так как нуль допускает счетную фундаментальную систему окрестностей, определенное таким образом топологическое кольцо E *метризуемо* (Общ. топол., гл. IX, § 3, предложение 1). Кроме того, оно *полное*, так как для всякой последовательности Коши (u_n) в кольце E и для любого числа q существует такое число $n_0(q)$, что при $m \geqslant n_0$ и $n \geqslant n_0$ ряд $u_m - u_n$ имеет порядок, больший q. Иначе говоря, члены, степень которых не превосходит q, одни и те же во всех формальных рядах u_n при $n \geqslant n_0(q)$. Пусть u — формальный ряд, у которого однородная часть степени q совпадает с однородной частью степени q всех рядов u_n с $n \geqslant n_0(q)$ (для всех $q \geqslant 0$). Очевидно, u является пределом последовательности (u_n).

Кольцо многочленов $A[X_1, X_2, \ldots, X_p]$ *всюду плотно* в кольце E, которое, следовательно, можно рассматривать как *замыкание* этого кольца многочленов. Понятие суммируемого семейства, определенное в кольце E в n° 4, совпадает в топологическом кольце E с понятием суммируемого семейства, определенного в произвольной абелевой топологической группе (Общ. топол., гл. III, § 4), а предложение 1 является частным случаем ассоциативности суммы (Общ. топол., гл. III, § 4, теорема 2). Лемма, следующая за предложением 6, показывает, что всякое дифференцирование кольца $A[X_1, X_2, \ldots, X_p]$ со значениями в кольце E *равномерно непрерывно*. Это позволяет передоказать предложение 6 топологически (см. Общ. топол., гл. II, § 3, теорема 1).

Упражнения. 1) Пусть I — произвольное множество индексов. Доказать, что аддитивный моноид $\mathbf{N}^{(I)}$ (§ 1, n° 1) удовлетворяет условию (D) главы II, § 7, n° 10. *Расширенная алгебра* этого моноида над коммутативным кольцом A, обладающим единицей, обозначается символом $A[[X_i]]_{i \in I}$ и называется также алгеброй *формальных рядов* с коэффициентами в A относительно переменных X_i. Порядок ненулевого формального ряда определяется как наимень-

шая из поляых степеней его ненулевых членов. Доказать, что если A — область целостности, то $A[[X]]_{i\in I}$ — тоже область целостности, и выполняется соотношение (3).

2) Пусть K — поле, $f=\dfrac{u}{v}$ — рациональная дробь, принадлежащая полю $K(X_1, X_2, \ldots, X_p)$, и $v(0, 0, \ldots, 0)\neq 0$. Доказать, что систему рядов $(0, 0, \ldots, 0)$ можно подставить в любую производную $D_1^{n_1}\ldots D_p^{n_p}f$ и что если $\Sigma\alpha_{n_1\ldots n_p}X_1^{n_1}\ldots X_p^{n_p}$ — разложеиие f в формальный ряд, то

$$D_1^{n_1}D_2^{n_2}\ldots D_p^{n_p}f(0, 0, \ldots, 0)=n_1!\ n_2!\ \ldots!\ n_p!\ \alpha_{n_1n_2\ldots n_p}$$

(«формула Тейлора»). Вывести отсюда разложение в формальный ряд рациональной дроби $1/(1-X)^p$.

*3) Пусть $u(X)=\sum_{n=0}^{\infty}\alpha_nX^n$ — формальный ряд над полем K.

а) Для того чтобы u был рациональной дробью в кольце $K(X)$, необходимо и достаточно, чтобы существовала конечная последовательность $(\lambda_i)_{1\leqslant i\leqslant q}$ элемеятов поля K, не все из которых равны нулю, и такое число $d\geqslant 0$, что для всех $n\geqslant d$

$$\lambda_1\alpha_n+\lambda_2\alpha_{n+1}+\ldots+\lambda_q\alpha_{n+q-1}=0.$$

б) Пусть

$$H_n^{(k)}=\begin{vmatrix}\alpha_n & \alpha_{n+1} & \ldots & \alpha_{n+k-1}\\ \alpha_{n+1} & \alpha_{n+2} & \ldots & \alpha_{n+k}\\ \alpha_{n+2} & \alpha_{n+3} & \ldots & \alpha_{n+k+1}\\ \alpha_{n+k-1} & \alpha_{n+k} & \ldots & \alpha_{n+2k-2}\end{vmatrix}$$

(«определитель Ханкеля»). Доказать, что если $H_{d+j}^{(q+1)}=0$ и $H_{d+j}^{(q)}\neq 0$ для всех $j\geqslant 0$, то $u(X)$ — рацнональнан дробь (использовать а)).

в) Доказать тождество

$$H_n^{(k)}H_{n+2}^{(k)}-H_n^{(k+1)}H_{n+2}^{(k-1)}=(H_{n+1}^{(k)})^2$$

(см. гл. III, § 8, упражнение 11). Вывести отсюда, что если $H_{m+j}^{(k+1)}=0$ при $0\leqslant j\leqslant r-1$, то определители $H_{m+j}^{(k)}$, $1\leqslant j\leqslant r$, либо все равны нулю, либо все не равяы нулю.

г) Вывести из б) и в) следующее утверждение. Для того чтобы ряд $u(X)$ был рациональной дробью, необходимо и достаточно, чтобы существовали два целых числа d и q такие, что $H_{d+j}^{(q+1)}=0$ для всех $j\geqslant 0$.

4) Пусть $a_1, a_2, \ldots, a_p$ — целые числа, большие нуля, α_n — число конечных последовательностей $(X_i)_{1\leqslant i\leqslant p}$ неотрицательных целых

чисел, удовлетворяющих уравнению

$$a_1x_1+a_2x_2+\ldots+a_px_p=n.$$

Доказать, что формальный ряд $\sum_{n=0}^{\infty}a_nX^n$ (над полем Q) является разложением рациональной дроби

$$\frac{1}{(1-X^{a_1})(1-X^{a_2})\ldots(1-X^{a_p})}.$$

5) Пусть F — конечное множество положительных чисел, β_n — число конечных последовательностей (x_i), состоящих из $\leqslant n$ членов множества F и удовлетворяющих условию $\sum_i x_i=n$. Доказать, что формальный ряд $\sum_{n=0}^{\infty}\beta_nX^n$ над Q является разложением рациональной дроби

$$\frac{1}{1-X^{a_1}-X^{a_2}-\ldots-X^{a_p}},$$

где $(a_i)_{1\leqslant i\leqslant p}$ — последовательность элементов из F, расположенных в порядке возрастания.

6) Пусть K — поле. Доказать, что в кольце формальных рядов $K[[X_1, X_2, \ldots, X_p]]$ существует только один максимальный идеал и он совпадает с множеством всех необратимых элементов. Доказать, что в кольце многочленов $K[X_1, X_2, \ldots, X_p]$, напротив, существует несколько различных максимальных идеалов.

7) Пусть K — поле. Доказать, что не существует формального ряда $u(X, Y)\in K[[X, Y]]$, для которого $(XY)^{-m}(X+Y)\,u(X, Y)=1$, m — любое положительное целое число.

8) Пусть K — поле, k — целое число, не кратное характеристике поля K. Доказать, что для любого формального ряда $u\in K[[X]]$, свободный член которого равен единице, существует формальный ряд $v\in K[[X]]$ такой, что $v^k=u$ (положить $v=1+w$).

*9) Пусть E — векторное пространство, имеющее бесконечный базис, над полем K характеристики 2. Пусть A — внешняя алгебра $\bigwedge E$ этого пространства, являющаяся коммутативным кольцом с единицей. Привести пример формального ряда $u\in A[[X]]$ такого, что $u^2=0$, но не существует элемента $\gamma\neq 0$, $\gamma\in A$, для которого $\gamma u=0$ (см. § 1, упражнение 11).

10) Пусть A — *не обязательно коммутативное* кольцо с единицей и σ — эндоморфизм A такой, что $\sigma(1)=1$. На аддитивной группе произведения $E=A^N$ определим внутренний закон композиции, положив $(\alpha_n)(\beta_n)=(\gamma_n)$, где $\gamma_n=\sum_{p+q=n}\alpha_p\sigma^p(\beta_q)$ $(\sigma^0(\xi)=\xi)$.

а) Доказать, что этот закон композиции ассоциативен и дистрибутивен с обеих сторон по отношению к сложению в E и, следовательно, определяет на E структуру кольца, имеющего в качестве единицы e последовательность (α_n), где $\alpha_0=1$, $\alpha_n=0$ при $n\geqslant 1$. Отображение, ставящее в соответствие всякому $\xi\in A$ элемент $(\alpha_n)\in E$ такой, что $\alpha_0=\xi$, $\alpha_n=0$ для $n\geqslant 1$, является изоморфизмом A на подкольцо кольца E, с которым мы отождествим A. Будем писать $\sum_{n=1}^{\infty}\alpha_n X^n$ вместо (α_n); тогда $X^p\beta=\sigma^p(\beta)X^p$ для любого элемента $\beta\in A$. Если ряд $u=\sum_{n=0}^{\infty}\alpha_n X^n$ отличен от нуля, то наименьшее число k, для которого $\alpha_k\neq 0$, называется *порядком* u и обозначается символом $\omega(u)$.

б) Пусть A — кольцо без делителей нуля, σ — некоторый изоморфизм кольца A на свое подкольцо. Доказать, что E — кольцо без делителей нуля и что $\omega(uv)=\omega(u)+\omega(v)$, если $u\neq 0$ и $v\neq 0$.

в) Для того чтобы ряд $u=\sum_{n=0}^{\infty}\alpha_n X^n$ был обратим, необходимо и достаточно, чтобы элемент α_0 был обратим в кольце A.

г) Предположим, что A — поле, σ — его автоморфизм. Доказать, что для кольца E существует тело левых частных (гл. I, § 3, упражнение 8) и что всякий ненулевой элемент этого тела F может быть однозначно записан в виде uX^{-h}, где u — элемент нулевого порядка кольца E.

°*11) а) Пусть A и B — две вполне упорядоченные части множества R (они обязательно счетны: см. Общ. топол., гл. IV, § 2, упражнение 1). Доказать, что множество $A+B$ вполне упорядочено и что для любого элемента $c\in A+B$ существует только конечное число пар (a, b) с условиями $a\in A$, $b\in B$ и $c=a+b$. (Для того чтобы доказать, что всякая непустая часть множества $A+B$ имеет наименьший элемент, следует рассмотреть его нижнюю грань в R.)

б) Пусть K — поле. В некотором пространстве K^R рассмотрим векторное подпространство E, образованное элементами (α_x) такими, что множество $x\in R$, для которых $\alpha_x\neq 0$, вполне упорядочено. Для двух произвольных элементов (α_x), (β_x) пространства E положим $(\alpha_x)(\beta_x)=(\gamma_x)$, где $\gamma_x=\sum_{y+z=x}\alpha_y\beta_z$ (сумма имеет смысл ввиду а)). Доказать, что этот закон композиции определяет вместе со сложением в E структуру *поля* на E. Элементы кольца E записывают также в виде $\sum_{t\in R}\alpha_t X^t$ и называют *формальными рядами с вполне упорядоченными экспонентами* и коэффициентами в K.

ГЛАВА V

ПОЛЯ *)

§ 1. Простые поля. Характеристика

1. Простые поля

Известно (гл. I, § 9, n° 2), что пересечение произвольного семейства *подполей* поля K является *подполем* поля K. В частности, пересечение P *всех* подполей поля K есть *наименьшее подполе* поля K; оно не содержит никаких подполей, отличных от него самого.

Определение 1. *Поле называется простым, если оно не содержит никаких подполей, отличных от него самого.*

Итак, всякое поле K содержит единственное простое поле P. Определим его структуру. Для этого заметим, что P, как всякое подполе поля K, содержит единицу e поля K (потому что из равенства $x^2 = x$ и $x \neq 0$ следует, что $x = e$ в K, см. гл. I, § 9, n° 2). Таким образом, P — подполе K, *порожденное* элементом e (можно сказать также, что P — подполе K, порожденное пустой частью ϕ поля K). Сначала рассмотрим *подкольцо* A поля K, порожденное единицей e. A содержит все элементы $n \cdot e$, где $n \in Z$, и так как эти элементы образуют кольцо, A совпадает с множеством их. С другой стороны, отображение $n \longrightarrow n \cdot e$ является представлением кольца Z целых чисел на A (гл. I, § 8 n° 8). Множество чисел $n \in Z$, для которых $n \cdot e = 0$, является

*) За исключением предложений 11 и 14 § 10, результаты, приводимые в §§ 10 и 11 и обоих приложениях, не используют результатов §§ 8 и 9. Читатель, интересующийся главным образом теорией Галуа и ее приложениями, может прямо перейти от § 7 к § 10.

идеалом (p) кольца Z, где $p \geqslant 0$—*характеристика* (гл. I, § 8, n° 8) поля K, и кольцо A изоморфно факторкольцу $Z/(p)$. Возможны два случая:

1° $p = 0$. Тогда A изоморфно Z. Так как $A \subset P$, P содержит поле отношений кольца A (гл. I, § 9, n° 4), которое изоморфно полю Q рациональных чисел. Так как P — простое поле, оно совпадает с полем отношений кольца A и, следовательно, изоморфно Q.

2° $p > 0$. Так как A содержится в поле, то оно не может содержать делителей нуля, следовательно, $Z/(p)$ не имеет делителей нуля. Это значит, что равенство $p = mn$ $(m > 0,\ n > 0)$ влечет $m \equiv 0 \pmod{p}$ или $n \equiv 0 \pmod{p}$, т. е. $m = p$ или $n = p$, следовательно, p — простое число (гл. I, § 8, n° 7).

Однако известно (гл. I, § 9, теорема 2), что для любого простого числа p кольцо $Z/(p)$ является полем. Следовательно, P совпадает с A и изоморфно $Z/(p)$. В итоге получаем:

Теорема 1. *Характеристика поля K равна нулю или простому числу. Если характеристика поля K равна нулю, то простое подполе поля K изоморфно полю Q рациональных чисел. Если характеристика поля K равна $p > 0$, то простое подполе поля K изоморфно полю $Z/(p)$ целых чисел по модулю p.*

Замечания. 1) При доказательстве теоремы 1 мы не пользовались коммутативностью поля K, следовательно, теорема 1 применима и к некоммутативным *телам*.

2) Всякое *подтело* тела K (не обязательно коммутативного) содержит простое подполе тела K и, следовательно, имеет *ту же характеристику*, что и тело K. Таким образом, всякое тело, содержащее тело K, имеет ту же характеристику, что и тело K.

3) Поле Q бесконечно, следовательно, все поля характеристики нуль бесконечны, а все конечные поля имеют ненулевую характеристику.

2. *Характеристическая экспонента*

Пусть дано поле K характеристики p. *Характеристической экспонентой* поля K мы будем называть число p, если $p > 0$, и число 1, если $p = 0$.

Предложение 1. *Если p — характеристическая экспонента поля K, то отображение $x \longrightarrow x^p$ является изоморфизмом поля K на некоторое его подполе.*

Очевидно, что $(xy)^p = x^p y^p$. Докажем, что

$$(x+y)^p = x^p + y^p. \tag{1}$$

При $p=1$ равенство очевидно. При $p>1$ имеем

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}, \text{ где } \binom{p}{0} = \binom{p}{p} = 1.$$

Остается доказать, что $\binom{p}{k} e = 0$ при $1 < k < p$.

Так как $k! \binom{p}{k} = p(p-1) \dots (p-k+1)$, то

$$(k!\, e)\left(\binom{p}{k} e\right) = p(p-1) \dots (p-k+1)\, e = 0.$$

Но $k!\, e = e(2e)(3e) \dots (ke)$ и $he \neq 0$ для $1 < h < p$, следовательно, $k!\, e \neq 0$, откуда $\binom{p}{k} e = 0$. Таким образом, отображение $x \longrightarrow x^p$ является представлением поля K в себя; так как оно ненулевое, оно является изоморфизмом K на свое подполе (гл. I, § 9, теорема 1).

Следствие. *Для любого целого числа $f>0$ отображение $x \longrightarrow x^{p^f}$ является изоморфизмом поля K на свое подполе.*

Это утверждение получается f-кратным последовательным применением предложения 1. Тем самым имеем тождество

$$\left(\sum_{i=1}^{n} x_i\right)^{p^f} = \sum x_i^{p^f}. \tag{2}$$

Замечания. 1) Формула (2) показывает, что для любого простого числа p и любого целого числа $f>0$ число $\dfrac{p^f!}{q_1!q_2!\dots!q_r!}$, где q_i—неотрицательные числа, отличные от p^f, и $\Sigma q_i = p^f$, *делится на* p.

2) Заметим, что предложение 1 и формула (1) перестают быть верными, если K—*некоммутативное* тело характеристики $p>0$.

Для любой части A поля K символом A^p мы будем обозначать в этой главе образ A при изоморфизме $x \longrightarrow x^p$. В частности, K^p означает *подполе* поля K, являющееся образом K при этом изоморфизме *).

*) Разумеется, нельзя смешивать множество A^p ни с произведением p множеств, совпадающих с A, ни с множеством произведений $x_1x_2 \dots x_p$ по p элементов, принадлежащих A.

Заметим, что при $p=1$ $K^p=K$ (см. § 7, n° 3).

Предложение 2. *Пусть E — поле, содержащее подполе K с характеристической экспонентой p. Для произвольной части A множества E имеем:* $(K[A])^p=K^p[A^p]$ *и* $(K(A))^p=K^p(A^p)$.

Это предложение является непосредственным следствием определений кольца $K[A]$ (гл. IV, § 2, n° 1) и поля $K(A)$ (гл. IV, § 3, n° 2). Действительно, если кольцо B содержит $K^p \bigcup A^p$ и содержится в $(K[A])^p$, то оно является образом при изоморфизме $x \longrightarrow x^p$ кольца C, содержащего $K \bigcup A$ и содержащегося в $K[A]$, следовательно, совпадающего с $K[A]$, т. е. $K^p[A^p]=(K[A])^p$. Так же доказывается, что $K^p(A^p)=(K(A))^p$.

Предложение 3. *Пусть E — поле, содержащее подполе K с характеристической экспонентой p. Если B — базис векторного пространства $K[A]$ над K, то B^p — система образующих векторного пространства $K[A^p]$ над K.*

Действительно, B^p — базис пространства $K^p[A^p]$ над полем K^p, $K^p[A^p]$ — система образующих пространства $K[A^p]$ над полем K. Так как $K^p \subset K$, то B^p — система образующих пространства $K[A^p]$ над K.

3. Характеризация многочленов с нулевой производной

Предложение 4. *Пусть K — поле характеристики p. Для того чтобы имели место тождества* $\frac{\partial f}{\partial x_i}=0$, $1 \leqslant i \leqslant n$, $f \in K \times [X_1, X_2, \ldots, X_n]$, *необходимо и достаточно, чтобы многочлен f принадлежал подкольцу $K[X_1^p, X_2^p, \ldots, X_n^p]$ кольца $K \times [X_1, X_2, \ldots, X_n]$.*

При $p=0$ это означает, что многочлен f сводится к *константе* $\alpha \in K$.

Предложение очевидно при $n=0$ (по определению $K[X_i]_{i \in \phi}$; см. гл. IV, § 1, n° 2). Доказательство будем вести индукцией по n. Пусть $f \in K[X_1, X_2, \ldots, X_n]$; тогда $f=\sum_k g_k X_n^k$, где $g_k \in K[X_1, X_2, \ldots, X_{n-1}]$. Из равенства $\frac{\partial f}{\partial X_i}=0$ для $1 \leqslant i \leqslant n-1$ вытекает, что $\frac{\partial g_k}{\partial X_i}=0$ для всех k и для $1 \leqslant i \leqslant n-1$. Следова-

тельно, по предположению индукции, $g_k \in K[X_1^p, X_2^p, \ldots, X_{n-1}^p]$. С другой стороны, $\sum k g_k X_n^{k-1} = \frac{\partial f}{\partial X_k} = 0$, следовательно, $k g_k = 0$ для всех k и, значит, $g_k = 0$ для всех k, не кратных p, что и требовалось доказать.

Упражнения. 1) Пусть A—кольцо без делителей нуля, не обязательно коммутативное и не обязательно с единицей. Доказать, что характеристика A (определяемая как число $m > 0$, для которого идеал (m) является анулятором A) равна нулю или простому числу. Если A содержит единицу, то A содержит подкольцо, изоморфное $Z/(m)$.

2) Пусть A—область целостности, $\mathfrak{P}$—простой идеал (гл. I, § 8, упражнение 13) кольца A. Если характеристика кольца A—простое число $p > 0$, то характеристика кольца $A/\mathfrak{P}$ тоже равна p. Если характеристика кольца A равна нулю, то характеристика кольца $A/\mathfrak{P}$ равна нулю в том случае, когда не существует такого простого числа p, что $pA \subset \mathfrak{P}$. В противном случае существует только одно простое число p, обладающее этим свойством; оно и является характеристикой кольца $A/\mathfrak{P}$. Доказать, что когда $A/\mathfrak{P}$—конечное кольцо, имеет место второй случай. Дать примеры обоих случаев (взять $A = Z$ и $A = K[X]$, K—поле характеристики нуль).

§ 2. Расширения

Пусть K—поле, содержащееся в поле L. Единицы полей K и L совпадают, следовательно, L может быть снабжено структурой алгебры над K (гл. II, § 7, п° 1). Назовем поле L, снабженное структурой алгебры над K, *расширением* K, оставляя термин *надполе* для L снабженного структурой поля без операторов*). Заметим, что всякое поле можно рассматривать как расширение его простого подполя.

Всякий раз, когда без уточнений мы будем говорить, что поле K, содержится в кольце L, мы будем подразумевать; что K есть *подполе* кольца L (иначе говоря, что структура поля *индуцируется* структурой кольца в L).

Пусть L и M—два надполя поля K такие, что $K \subset L \subset M$. Назовем L *промежуточным полем* между K и M. Снабженное структурой расширения поля K, L являются подалгеброй M,

*) Таким образом, мы изменим смысл слова «расширение», которое мы определили в гл. I, § 9, п° 2 как синоним надполя.

которую мы будем также называть *подрасширением* расширения M поля K.

Замечание. Для того чтобы сделать более ясной ситуацию, в которой фигурируют несколько полей, мы будем использовать иногда диаграммы приведенного ниже вида (рис. 1).

$$\begin{array}{ccccc} & & M & \longrightarrow & P \\ & & \uparrow & & \uparrow \\ K & \longrightarrow & L & \longrightarrow & N \end{array}$$

Рис. 1.

Стрелка, идущая от одной буквы к другой, означает, что поле, обозначенное первой буквой, является подполем поля обозначенного второй буквой (таким образом, стрелка заменяет знак включения). Например, в диаграмме мы имеем $K \subset L$, $L \subset M \subset P$ и $L \subset N \subset P$.

1. Структура расширения

Расширение E поля K, будучи алгеброй над K, в частности снабжено структурой векторного пространства над K, размерность которого называется *степенью* расширения E (или еще *степенью надполя E относительно поля K*; см. гл. II, § 7, n° 2). Напомним (см. там же), что эту степень, когда она *конечна*, обозначают $[E:K]$. Символ $[E:K]$ определен только в этом случае.

Пусть E — расширение поля K, F — расширение поля E, $(\alpha_\lambda)_{\lambda \in L}$ — базис E над K, $(b_\mu)_{\mu \in M}$ — базис F над E. Тогда семейство $(b_\mu a_\lambda)_{(\mu, \lambda) \in M \times L}$ составляет базис F над полем K (гл. II, § 5, предложение 1). В частности (гл. II, § 5, следствие из предложения 1), получаем следующий результат:

Теорема 1. *Пусть E — расширение поля K, F — расширение поля E. Если хотя бы одно из чисел $[F:K]$, $[F:E]\cdot[E:K]$ определено, то определено и другое, и*

$$[F:K] = [F:E]\cdot[E:K].$$

Следствие 1. *Если F — расширение поля K конечной степени, E — промежуточное поле между K и F, то степени $[E:K]$ и $[F:E]$ являются делителями $[F:K]$.*

Тем самым, если степень $[F:K]$ — *простое* число, то не существует никаких подрасширений F, кроме K и F. Однако заметим, что если число $[F:K]$ не простое, то не обязательно существует подрасширение F, отличное от K и F (см. § 10, упражнение 7).

Следствие 2. *Если F — расширение конечной степени поля K, E — промежуточное поле между K и F, то равенство $[E:K]=[F:K]$ равносильно совпадению $E=F$*, а равенство $[F:E]=[F:K]$ *равносильно совпадению $E=K$.*

Действительно, если степень расширения поля K равна 1, то это расширение совпадает с K.

Предложение 1. *Пусть A — коммутативная алгебра с единицей e над полем K, имеющая конечный ранг над K. Если элемент $a\in A$ не является делителем нуля в A, то он обратим в A.*

Действительно, отображение $x\to ax$ является взаимно однозначным эндоморфизмом структуры векторного пространства на A, следовательно, оно — автоморфизм A с той же структурой (гл. III, следствие предложения 11), поэтому существует такой элемент $b\in A$, что $ab=e$.

Следствие. *Всякая область целостности A* (гл. I, § 8, n° 3), *содержащая поле K, имеет ту же единицу, что K. Если A, как алгебра над K, имеет конечный ранг над K, то A — поле.*

Действительно, пусть e — единица K, тогда $e^2=e$, откуда $e(x-ex)=0$ для всех $x\in A$, и так как $e\neq 0$, имеем $x=ex$, что доказывает первую часть следствия. Вторая часть непосредственно получается из предложения 1.

Пусть E и F — два расширения одного и того же поля K. В соответствии с общими определениями (см. гл. II, § 7, n° 4) *представление* расширения E в расширение F есть представление f структуры *поля* E в структуру поля F такое, что $f(zx)=zf(x)$ для $x\in E$ и $z\in K$ (мы рассматриваем только ненулевые представления, для которых $f(1)=1$). Это равносильно утверждению, что $f(z)=z$ (иначе говоря, z *инвариантно* относительно f) для всех $z\in K$. Так как представление f ненулевое, оно является *изоморфизмом* структуры поля E на структуру поля некоторого подполя поля F (содержащего K). Назовем f *K-изоморфизмом* поля E в поле F. Поля E и F будут называться *K-изоморфными*, если существует *K-изоморфизм* E на F. K-изоморфизм расширения E поля K на подрасширение поля E называется *K-эндо-*

морфизмом поля E и *K-автоморфизмом* поля E, если он отображает E на себя. Заметим, что для произвольного эндоморфизма u поля K множество элементов этого поля, *инвариантных* относительно u, является *подполем* K поля L (гл. II, § 5, n° 6), следовательно, u есть *K-эндоморфизм* поля L.

В частности, если P—простое подполе поля L, все эндоморфизмы поля L являются P-эндоморфизмами. Простое поле обладает только одним эндоморфизмом—тождественным.

2. Присоединение

Пусть E—надполе поля K. Напомним, что для заданного семейства $x=(x_\iota)_{\iota\in I}$ элементов поля E (гл. IV, § 3, n° 2) символом $K(x_\iota)_{\iota\in I}$ (или $K(\boldsymbol{x})$, или еще $K(x_1, \ldots, x_n)$, когда I—интервал $[1, n]$ множества N) мы обозначаем наименьшее подполе поля E, содержащее K и элементы семейства (x_ι). Будем говорить, что поле $K(x_\iota)_{\iota\in I}$ получается *присоединением* к K элементов семейства $(x_\iota)_{\iota\in I}$ и что семейство (x_ι) (или множество его элементов) является *системой образующих* поля $K(x_\iota)_{\iota\in I}$ *относительно* K (или над K). Поле $K(x_\iota)_{\iota\in I}$ зависит только от множества A элементов семейства (x_ι); напомним, что оно обозначается также символом $K(A)$. В частности, $K(E)=E$ и $K(\phi)=K$.

Предложение 2. *Пусть M и N—две произвольные части надполя E поля K; тогда* $K(M\cup N)=K(M)(N)=K(N)(M)$.

Действительно, поле $K(M\cup N)$ содержит поле $K(M)$ и множество N, а следовательно, и поле $K(M)(N)$. Так как поле $K(M)(N)$ содержит множество $K\cup M\cup N$, то оно содержит также $K(M\cup N)$, откуда следует требуемое.

Иногда пишут $K(M, N)$ вместо $K(M\cup N)$.

Замечание. Если P—простое подполе поля E (§ 1), то для любой части A поля E $P(A)$—наименьшее подполе, содержащее A. В частности, если K—подполе поля E, то $P(K\cup A)=K(A)$. Если K и K'—подполя поля E, то $P(K\cup K')=K(K')=K'(K)$. Это поле является наименьшим подполем поля E, содержащим K и K', или *верхней гранью* полей K и K' в множестве подполей поля E, упорядоченных по включению.

Предложение 3. *Пусть $\mathfrak{F}$—множество подполей поля E, фильтрующееся по отношению $\subset$; тогда объединение L полей множества $\mathfrak{F}$ есть поле.*

Действительно, если x, y — элементы множества L, то существуют поля R, S, принадлежащие множеству $\mathfrak{F}$ и такие, что $x \in R$, $y \in S$. Пусть T — поле из множества $\mathfrak{F}$, содержащее поля R и S; Тогда $x \in T$, $y \in T$, следовательно $x+y$, xy и x^{-1} (если $x \neq 0$) принадлежат T и, следовательно, L *).

Следствие. *Пусть K — подполе поля E. Поле $K(A)$, получающееся присоединением к K некоторой части A поля E, является объединением полей $K(F)$, где F пробегает множество конечных частей множества A.*

Действительно, множество полей $K(F)$ на основании предложения 2 фильтруется по отношению $\subset$. Следовательно, объединение L этих полей является полем, содержащим $K \bigcup A$ и содержащимся в поле $K(A)$ и, следовательно, совпадающим с $K(A)$.

Определение 1. *Расширение E поля K называется расширением конечного типа, если оно обладает конечной системой образующих. Оно называется простым, если оно обладает системой образующих, сводящейся к одному элементу.*

Следствие к предложению 3 показывает, что всякое расширение E поля K является объединением расширений конечного типа, содержащихся в E. Ясно, что всякое расширение E поля K *конечной степени* является расширением *конечного типа*, так как база E (рассматриваемого как векторное пространство над K) является системой образующих поля E над K. Позже мы увидим, что обратное утверждение неверно.

3. *Линейно разделенные расширения*

Пусть Ω — расширение поля K, A и B — подкольца поля Ω, содержащие K; тогда их можно рассматривать как *подалгебры* алгебры Ω (над полем K). Пусть C — подкольцо поля Ω, *порож-*

*) Принцип этого доказательства приложим к более общему случаю, когда E обладает алгебраической структурой $\mathcal{S}$; $\mathfrak{F}$ — множество, фильтрующееся по отношению $\subset$, частей E, на которых $\mathcal{S}$ индуцирует ту же структуру, и в аксиомах структуры $\mathcal{S}$ участвуют только *конечные* части множества, на котором она определена. На объединении L множеств из $\mathfrak{F}$ структура $\mathcal{S}$ индуцирует ту же структуру $\mathcal{S}$. Например, можно брать в качестве $\mathcal{S}$ структуру группы с операторами, или кольца с операторами, или алгебраически замкнутого поля, или совершенного поля и т. д.

денное множеством $A \bigcup B$. Напомним, что существует представление φ *тензорного произведения* $A \otimes B$ алгебр A и B над полем K на алгебру C, ставящее в соответствие каждому тензорному произведению $x \otimes y (x \in A,\ y \in B)$ произведение xy, лежащее в C (гл. III, § 3, п° 3). Иначе говоря, если (b_μ)—базис алгебры B над полем K, (a_λ)—базис алгебры A над полем K, то алгебра C отождествляется с множеством линейных комбинаций $\sum_\mu \alpha_\mu b_\mu$, где $\alpha_\mu \in A$, множеством $\sum_\lambda \beta_\lambda a_\lambda$, где $\beta_\lambda \in B$, а также множеством $\sum_{\lambda,\,\mu} \gamma_{\lambda\mu} a_\lambda b_\mu$, где $\gamma_{\lambda\mu} \in K$. Напомним еще, что алгебры A и B называются *линейно разделенными* над K, если представление φ является *изоморфизмом* $A \otimes B$ на C. В этом случае $A \bigcap B = K$ и всякая независимая над K часть алгебры B (соответственно A) является независимой над A (соответственно B). Обратно, для того чтобы A и B были линейно разделены над K, достаточно существования базиса алгебры B над K (например), который независим над A (гл. III, § 3, теорема 1).

Разберем в частности случай, когда A и B являются *подрасширениями* поля Ω.

Предложение 4. *Пусть E и F—расширения поля K, содержащиеся в расширении Ω.*

а) *Пусть F—расширение конечной степени поля K; тогда подкольцо расширения Ω, порожденное множеством $E \bigcup F$, является полем, совпадающим с $E(F)$, степень которого относительно E конечна. Далее, $[E(F) : E] \leqslant [F : K]$, и равенство $[E(F) : E] = [F : K]$ имеет место в том и только в том случае, когда поля E и F линейно разделены над K.*

б) *Если, кроме того, E имеет конечную степень над K, то $E(F) = K(E \bigcup F)$, и это поле имеет конечную степень над K. Тогда $[K(E \bigcup F) : K] \leqslant [E : K]\,[F : K]$, и равенство $[K(E \bigcup F) : K] = [E : K]\,[F : K]$ выполняется в том и только в том случае, когда E и F линейно разделены над K.*

Действительно, пусть C—подкольцо расширения Ω, порожденное множеством $E \bigcup F$. Пусть, далее, $(b_j)_{1 \leqslant j \leqslant n}$—базис F над K; тогда C отождествляется с векторным пространством над E, порожденным элементами b_j, следовательно, C—алгебра *конечного* ранга, не превосходящего n, над полем E. Так как C

содержится в некотором поле и, следовательно, является областью целостности, то C — *поле* (следствие предложения 1). Отсюда следует, что $C = E(F)$ и $[E(F):E] \leqslant [F:K]$. Равенство $[E(F):E] = [F:K]$ означает, что элементы b_j линейно независимы над E, и следовательно, поля E и F линейно разделены над K. Часть а) предложения доказана. Часть б) тотчас следует из части а), так как $[E(F):K] = [E(F):E][E:K]$.

Если E и F — расширения поля K бесконечной степени, содержащиеся в Ω, то подкольцо C, порожденное множеством $E \cup F$, не обязано быть полем (упражнение 1), однако *поле частных* кольца C совпадает с $K(E \cup F)$. В более общем случае, когда A — такое подкольцо E, что E совпадает с полем частных кольца A, а B — такое подкольцо F, что F совпадает с полем частных кольца B, наконец, C — подкольцо поля Ω, порожденное множеством $A \cup B$, тогда поле $K(E \cup F)$ совпадает с полем частных кольца C, так как оно является наименьшим подполем поля Ω, содержащим C, E и F. Кроме того, мы имеем

Предложение 5. *Пусть E и F — расширения поля K, содержащиеся в Ω. A и B — подкольца кольца Ω, содержащие K и такие, что E — поле частных кольца A, а F — поле частных кольца B. Для того чтобы поля E и F были линейно разделены над K, необходимо и достаточно, чтобы кольца A и B были линейно разделены над K.*

Условие, очевидно, необходимо. Обратно, если A и B линейно разделены над K, то линейно разделены кольца A и F, так как, если семейство элементов поля Ω независимо относительно B, то оно независимо относительно поля частных F кольца B (гл. III, § 2, предложение 5). То же рассуждение показывает затем, что поля E и F линейно разделены над K.

Предложение 6. *Пусть E и F — расширения поля K, содержащиеся в Ω. Если E и F линейно разделены над K, то всякое подрасширение расширения E и всякое подрасширение расширения F линейно разделены над K. Обратно, если всякая пара подрасширений конечного типа E' и F' расширений E и F соответственно линейно разделена над K, то E и F линейно разделены над K.*

Действительно, условие линейной разделенности расширений E и F можно выразить следующим образом: если (a_α) — произ-

вольное независимое семейство элементов расширения E и (b_β) — произвольное независимое семейство элементов расширения F, то из соотношения $\sum_{\alpha,\beta} \lambda_{\alpha\beta} a_\alpha b_\beta = 0$, где $\lambda_{\alpha\beta} \in K$, должны вытекать равенства $\lambda_{\alpha\beta} = 0$ (для всех пар индексов $\alpha\beta$). Но это условие выполняется для любой пары независимых семейств, если оно выполняется для любой пары конечных независимых семейств.

Образно говоря, линейная разделенность является свойством «конечного характера».

Предложение 7. *Пусть E, F, G — расширения поля K, содержащиеся в расширении Ω поля K, и пусть $F \subset G$. Для того чтобы поля E и G были линейно разделены над K, необходимо и достаточно, чтобы поля E и F были линейно разделены над K, а поля $E(F)$ и G были линейно разделены над F.*

Условие необходимо, так как, если E и G линейно разделены над K, то E и F линейно разделены над K (предложения 6). С другой стороны, всякий базис (a_α) поля E над K является одновременно базисом алгебры $F[E]$ над полем F. Так как, по предположению, семейство (a_α) независимо относительно G, то алгебры $F[E]$ и G линейно разделены над F, а следовательно, линейно разделены и поля $E(F) = F(E)$ и G (предложение 5).

Условие достаточно, так как при тех же обозначениях оно влечет независимость семейства (a_α) над полем F; следовательно, (a_α) составляет базис алгебры $F(E)$ над F. По предположению, $F(E)$ и G линейно разделены над F, следовательно, семейство (a_α) независимо над G. Отсюда следует линейная разделенность полей E и G над K.

Упражнения. 1) В поле $K(X, Y)$ рациональных дробей от двух переменных над полем K доказать, что $K(X)$ и $K(Y)$ — линейно разделенные расширения поля K, но подкольцо поля $K(X, Y)$, порожденное множеством $K(X) \cup K(Y)$, отлично от $K(X, Y)$ (см. § 9, упражнение 4).

2) Пусть A — произвольная алгебра над полем K, имеющая конечный ранг над K, и пусть элемент $a \in A$ не является делителем нуля слева. Доказать, что существует такой элемент $e \in A$, что $ex = x$ для всех $x \in A$, и такой элемент $b \in A$, что $ab = e$ (см. гл. I, § 2, упражнение 9). Вывести отсюда, что если A имеет конечный ранг над K и не содержит делителей нуля, то A — тело (не обязательно коммутативное).

§ 3. Алгебраические расширения

1. Алгебраические элементы

Пусть K — поле, E — расширение поля K, $x \in E$. Мы будем изучать подкольцо $K[x]$ поля E, порожденное x и K (гл. IV, § 2, n° 1). Это кольцо является *областью целостности*, изоморфной $K[X]/\mathfrak{a}$, где $\mathfrak{a}$ — идеал алгебраических соотношений с коэффициентами из K, которым удовлетворяет элемент x (или модуль линейных соотношений с коэффициентами из K между одночленами x^n ($n \in \mathbf{N}$): см. гл. IV, § 2, теорема 1). В зависимости от того, равен (0) идеал $\mathfrak{a}$ или нет, могут представиться два случая.

Определение 1. *Элемент x расширения E поля K называется трансцендентным над K, если идеал $\mathfrak{a}$ алгебраических соотношений с коэффициентами из K, которым удовлетворяет элемент x, есть* (0) (*или, что то же, если одночлены x^n ($n \in N$) линейно независимы над K*). *В противном случае элемент x называется алгебраическим над K.*

Утверждение, что x алгебраичен над K, означает таким образом, что существуют элементы α_i, принадлежащие полю K и не все равные нулю ($0 \leqslant i \leqslant n$) такие, что $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n = 0$.

Если идеал $\mathfrak{a}$ ненулевой, то, как известно (гл. IV, § 1, предложение 7), он является главным идеалом (f) в кольце $K[X]$; многочлен f, если считать его унитарным, определяется однозначно. Пусть n — степень f; тогда классы по модулю (f) элементов X^k ($0 \leqslant k \leqslant n-1$) образуют базис алгебры $K[X]/(f)$ над полем K (гл. IV, § 1, предложение 4). Так как кольцо $K[X]/(f)$, изоморфное кольцу $K[x]$, является областью целостности и имеет конечный ранг над K, то оно — поле (§ 2, следствие из предложения 1). Следовательно, (f) — максимальный идеал и f — *неприводимый* многочлен; кроме того, так как $K[x]$ — поле, то оно совпадает, по определению, с $K(x)$ и имеет конечную степень над K.

Определение 2. *Пусть x — алгебраический над K элемент расширения E поля K; число $[K(x):K]$ называется степенью элемента x над K.*

В частности, для того чтобы алгебраический над K элемент принадлежал K, необходимо и достаточно, чтобы его степень над K была равна 1.

Таким образом мы доказали следующую теорему:

Теорема 1. а) *Для того чтобы элемент x расширения E поля K был алгебраическим над K, необходимо и достаточно, чтобы кольцо $K[x]$ было алгеброй конечного ранга над K; тогда это кольцо совпадает с полем $K(x)$.*

б) *Если x имеет степень n над K, то существует единственный унитарный многочлен $f \in K[X]$ степени n такой, что $f(x) = 0$.*

в) *Многочлен f неприводимый. Множество многочленов $g \in K[X]$ таких, что $g(x) = 0$, является главным идеалом (f).*

г) *Отображение $g \to g(x)$ является гомоморфизмом кольца $K[X]$ на поле $K(x)$. Поле $K(x)$ изоморфно полю $K[X]/(f)$, и элементы $1 = x^0, x, x^2, \ldots, x^{n-1}$ образуют базис $K(x)$ над K.*

Определение 3. *Пусть x — алгебраический над K элемент расширения E поля K; минимальным многочленом элемента x над K будем называть единственный унитарный неприводимый многочлен $f \in K[X]$, для которого $f(x) = 0$.*

Это равносильно утверждению, что f — унитарный многочлен кольца $K[X]$ степени, равной степени элемента x над K и такой, что $f(x) = 0$.

Таким образом, всякий неприводимый унитарный многочлен кольца $K[X]$ является минимальным многочленом каждого из своих корней во всяком расширении E поля K (если у него вообще есть корни в расширении E).

Корни неприводимого многочлена $f \in K[X]$ в расширении E поля K не обязаны быть *простыми*. Точнее, справедливо следующее утверждение:

Предложение 1. *Пусть K — поле характеристики p, x — алгебраический над K элемент расширения E поля K. Для того чтобы x был простым корнем своего минимального многочлена f над K, необходимо и достаточно, чтобы f не принадлежал кольцу $K[x^p]$.*

Действительно, для того чтобы x был кратным корнем многочлена f, необходимо и достаточно, чтобы $f'(x) = 0$ (гл. IV, § 4, предложение 3). Следовательно, многочлен f' должен делиться на f (теорема 1). Это возможно только при $f' = 0$, так как в противном случае мы имеем $\deg f' < \deg f$ и f' не может быть кратным f. Так как условие $f' = 0$ эквивалентно включению $f \in K[x^p]$ (§ 1, предложение 4), предложение доказано.

Следствие 1. *Пусть K — поле характеристики* нуль, *E — произвольное расширение поля K, f — неприводимый многочлен кольца $K[X]$; тогда все корни многочлена f в E простые.*

Примеры.° 1) В поле комплексных чисел C число i алгебраическое и имеет степень 2 над простым полем Q. Действительно, если $f(x)=x^2+1$, то $f(i)=0$, но $x^2+1\neq 0$ ни для одного числа $x\in Q$, следовательно, $i\notin Q$. Поле $Q(i)$ является расширением степени 2 поля Q, оно состоит из чисел $a+bi$, где a и b — рациональные. ₀ 96

2) Пусть K — поле, F — поле $K(X)$ рациональных дробей от одной переменной над K. Пусть E — подполе $K(X^3)$ поля F; тогда $F=E(X)$ и элемент X — алгебраичен над E, так как он является корнем многочлена Y^3-X^3 кольца $E[Y]$. Этот многочлен неприводим в кольце $E[Y]$, ибо в противном случае он имеет по крайней мере один множитель первой степени, и, следовательно, существуют два ненулевых многочлена u и v кольца $K[X]$ такие, что $(u(X))^3=$ $=X^3(v(X^3))^3$. Это невозможно, потому что, обозначая буквами m и n степени многочленов u и v, соответственно получаем $9m=9n+3$ или $3m=3n+1$. Следовательно, поле F является расширением степени 3 поля E, и всякий элемент поля F можно записать единственным образом в виде $f(X^3)+Xg(X^3)+X^2h(X^3)$, где f, g, h — рациональные дроби, принадлежащие $K(X)$.

Если K имеет *характеристику* 3, то неприводимый многочлен Y^3-X^3 принадлежит кольцу $E[Y^3]$ и, следовательно (предложение 1), его корни в F *кратные*. Впрочем легко видеть, что X — *единственный* корень этого многочлена в поле F, так как в поле характеристики p равенство $x^p=y^p$ влечет $x=y$ (§ 1, предложение 1).

°3) В поле R действительных чисел можно доказать *), что число π *трансцендентно* над простым полем Q (см. упражнение 1).₀

Предложение 2. *Пусть E — расширение поля K, x — элемент E, алгебраический над K. Для любого поля F, промежуточного между K и E, элемент x алгебраичен над F, его минимальный многочлен над F делит минимальный многочлен x над K, а степень x над F не превосходит степени x над K.*

Действительно, пусть f — минимальный многочлен элемента x над K. Поскольку $f(x)=0$ и $f\in F[X]$, x алгебраичен над F и, следовательно, f кратен минимальному многочлену элемента x над полем F (теорема 1 в)).

---

*) См., например, D. Hilbert, Gesammelte Abhandlungen, Berlin (Springer), 1932, t. I, p. 1

Замечание. Пусть A — коммутативная алгебра над полем K, обладающая той же единицей, что и K (которая, следовательно, содержится в A). Определение 1 применимо без изменений к произвольному элементу x алгебры A. Если элемент x алгебраичен над K, то идеал $\mathfrak{a}$ алгебраических соотношений с коэффициентами в K, которым удовлетворяет элемент x, является главным идеалом (f), где f — унитарный многочлен кольца $K[X]$, который, вообще говоря, не обязан быть неприводимым. Подалгебра $K[x]$ алгебры A изоморфна кольцу $K[X]/(f)$, и если f имеет степень n, то элементы $1, x, x^2, \ldots, x^{n-1}$ образуют базис алгебры $K[x]$ над K. Заметим, что если $f = \sum_{k=0}^{n} a_k X^k$ и если $a_0 \neq 0$, то $-1 = x \sum_{k=1}^{n} a_0^{-1} a_k x^k$, следовательно, x *обратим* в $K[x]$ и $x^{-1} = -\sum_{k=1}^{n} a_0^{-1} a_k x^k$.

2. *Алгебраические расширения*

Определение 4. *Расширение E поля K называется алгебраическим* (или надполе E поля K называется алгебраическим над K, или еще, что то же, расширение E является алгебраическим *над* K), *если всякий элемент расширения E является алгебраическим над K. Расширение E поля K, не являющееся алгебраическим, называется трансцендентным* (над K).

Предложение 3. *Для того чтобы расширение E поля K было алгебраическим, необходимо и достаточно, чтобы всякое кольцо A, для которого $K \subset A \subset E$, было полем.*

Условие необходимо, так как если E — алгебраическое расширение поля K и $x \neq 0$ — элемент кольца A, то подкольцо $K[x]$ кольца A совпадает с полем $K(x)$ (теорема 1а)), следовательно, элемент x обратим в A, т. е. A — поле. Условие достаточно; если оно выполнено и x — произвольный ненулевой элемент расширения E, то кольцо $K[x]$ представляет собой поле, следовательно, $x^{-1} \in K[x]$, т. е. (гл. IV, § 2, предложение 1) существует многочлен $g \in K[X]$ такой, что $x^{-1} = g(x)$. Тем самым $xg(x) - 1 = 0$, что означает алгебраичность x над полем K; следовательно, E — алгебраическое расширение поля K.

Предложение 4. *Если расширение E поля K имеет конечную степень n, то оно алгебраическое, и степень над K произвольного элемента расширения E делит n.*

Действительно, для любого $x \in E$ число $[K(x):K]$ конечно и делит n (§ 2, следствие 1 из теоремы 1), и следовательно, элемент x алгебраичен над K.

Утверждение, обратное этому предложению, неверно; позже (§ 4, п° 2) мы дадим пример алгебраического расширения бесконечной степени.

Предложение 5. *Пусть $E = K(a_1, a_2, \ldots, a_m)$ — расширение поля K конечного типа и пусть все элементы a_i $(1 \leqslant i \leqslant m)$ алгебраичны над K. Тогда E — расширение поля K конечной степени. Пусть n_i — степень элемента a_i над полем $K(a_1, a_2, \ldots, a_{i-1})$; тогда степень поля E над K равна $n_1 n_2 \ldots n_m$, и элементы $a_1^{\nu_1} a_2^{\nu_2} \ldots a_m^{\nu_m}$ $(0 \leqslant \nu_i \leqslant n_{i-1})$ образуют базис расширения E поля K.*

Действительно, элементы $a_i^{\nu_i}$ $(0 \leqslant \nu_i \leqslant n_{i-1})$ образуют базис поля $K(a_1, a_2, \ldots, a_i)$ над $K(a_1, a_2, \ldots, a_{i-1})$ (теорема 1г)). Предложение непосредственно получается индукцией по m из предложения I гл. II, § 5 (см. § 2, п° 1).

Замечания. 1) Мы имеем $E = K[a_1, a_2, \ldots, a_m]$, и, следовательно, поле E изоморфно факторкольцу $K[X_1, X_2, \ldots, X_m]/\mathfrak{a}$, где $\mathfrak{a}$ — идеал алгебраических соотношений между элементами a_i с коэффициентами из K (гл. IV, § 2, теорема 1); так как E — поле, то $\mathfrak{a}$ — *максимальный* идеал кольца $K[X_1, \ldots, X_m]$.

2) Пусть E — алгебраическое расширение поля K бесконечной степени. Из предложения 5 следует существование бесконечной последовательности (a_n) элементов E таких, что $a_n \notin K(a_1, a_2, \ldots, a_{n-1})$. Кроме того, предложение 5 показывает, что степень поля $K(a_1, a_2, \ldots, a_n)$ над K может принимать как угодно большие значения. Иначе говоря, если E — такое алгебраическое расширение поля K, что степени $[F:K]$ подрасширений конечной степени поля E *ограничены*, то E — расширение *конечной* степени поля K.

Предложение 6. *Пусть E — расширение поля K, A — часть E, состоящая из алгебраических над K элементов; тогда $K(A)$ — алгебраическое расширение поля K.*

Действительно, всякий элемент x, принадлежащий $K(A)$, принадлежит полю $K(F)$, где F — конечная часть A (§ 2, следствие из предложения 3); расширение $K(F)$ алгебраично над K (предложение 5), следовательно, элемент x алгебраический над K.

Предложение 7. *Пусть Ω — некоторое расширение поля K, E и F — расширения K, содержащиеся в Ω. Если расширение F*

алгебраично над K, то подкольцо C, порожденное множеством $E \cup F$, является полем, которое совпадает с $E(F)$ и алгебраично над E.

Действительно, всякий элемент расширения F, будучи алгебраичным над K, алгебраичен над F (предложение 2), следовательно (предложение 6), $E(F)$ — алгебраическое расширение поля E. Так как C — кольцо, содержащееся в $E(F)$ и содержащее E, то C — поле (предложение 3), следовательно, оно совпадает с $E(F)$ ввиду определения последнего.

3. Транзитивность алгебраических расширений. Поля, алгебраически замкнутые внутри своего расширения

Предложение 8. *Пусть E и F — два надполя поля K и $K \subset E \subset F$. Для того чтобы поле F было алгебраическим над K, необходимо и достаточно, чтобы E было алгебраическим над K, а F алгебраическим над E.*

Условие необходимо ввиду предложения 2. Докажем, что оно достаточно. Пусть x — произвольный элемент расширения F; он алгебраичен над E; пусть $g \in E[X]$ — минимальный многочлен элемента x над E. Обозначим символом A множество (конечное) коэффициентов многочлена g; элемент x алгебраичен над полем $K(A)$. Так как расширение $K(A)$ имеет конечную степень над K (предложение 5), а расширение $K(A \cup \{x\}) = K(A)(x)$ имеет конечную степень над $K(A)$, то (§ 2, теорема 1) расширение $K(A \cup \{x\})$ имеет конечную степень над K и, значит, элемент x алгебраичен над K (предложение 4).

Определение 5. *Подполе K поля E называется алгебраически замкнутым в E, если всякий элемент расширения E, алгебраический над K, принадлежит K.*

Это равносильно утверждению, что K — единственное алгебраическое расширение поля E, содержащееся в E. Всякое поле является алгебраически замкнутым в себе. В § 4 мы изучим поля, алгебраически замкнутые в любом надполе.

Предложение 9. *Пусть E — произвольное надполе поля K. Множество L тех элементов поля E, которые алгебраичны над K, составляет поле, алгебраически замкнутое в E.*

Действительно (предложение 6), поле $K(L)$ алгебраично над K, следовательно, $K(L) \subset L$, и, значит, $K(L) = L$ и L — поле. С другой стороны, если элемент $x \in E$ алгебраичен над L, то он алгебраичен над K (предложение 8) и, следовательно, принадлежит L.

Расширение L поля K, состоящее из элементов E, алгебраичных над K, называют *алгебраическим замыканием поля K в E*. Оно является *наибольшим алгебраическим расширением поля K*, содержащимся в E.

Упражнения. 1) Доказать, что всякое алгебраическое расширение E поля K равномощно части множества $K \times N$ (рассмотреть отображение, ставящее в соответствие каждому элементу из E его минимальный многочлен над K; использовать тот факт, что множество конечных частей бесконечного множества A равномощно A). В частности, всякое алгебраическое расширение конечного поля счетно и всякое алгебраическое расширение бесконечного поля K равномощно K. °Вывести отсюда, что в поле R действительных чисел существуют трансцендентные над простым полем Q числа и что множество их имеет мощность континуума. ∘

2) Пусть E — расширение поля K, x и y — два различных корня одного и того же неприводимого многочлена кольца $K[X]$, $x, y \in E$. Доказать, что расширения $K(x)$ и $K(y)$ не являются линейно разделенными над K (использовать предложение 4 а), § 2). °Если в качестве K взять Q, в качестве E поле C комплексных чисел, в качестве x действительный корень и в качестве y комплексный корень многочлена $x^3 - 2$, то доказать, что $K(x) \cap K(y) = K$. ∘

3) Пусть (E_ι) — семейство расширений поля K, содержащихся в расширении G поля K. Пусть F_ι — алгебраическое замыкание поля K в E; доказать, что алгебраическое замыкание поля K в $E = \bigcap_\iota E_\iota$ есть $F = \bigcap_\iota F_\iota$.

* 4) Пусть K — поле, A — подкольцо поля K, $L \subset K$ — поле частных кольца A.

а) Доказать, что если K есть A-модуль, допускающий конечную систему образующих, то $L = A$. (Полагая $K = \sum_{i=1}^{n} Ac_i$, доказать, что L есть A-модуль с конечным числом образующих, разлагая K, рассматриваемое как векторное пространство над L, в прямую сумму L и некоторого дополнительного подпространства.)

б) Доказать, что если существует конечное число элементов x_i поля K алгебраичных над L и таких, что $K = A[x_1, \ldots, x_n]$, то существует отличный от нуля элемент $b \in A$ такой, что $L = A\left[\frac{1}{b}\right]$

(доказать существование элемента $b \in A$ такого, что K является $A\left[\frac{1}{b}\right]$-модулем с конечным числом образующих). Вывести отсюда, что b принадлежит всем максимальным идеалам кольца A.

§ 4. Алгебраически замкнутые расширения

1. *Алгебраически замкнутое поле*

Предложение 1. *Для любого поля K следующие четыре свойства эквивалентны.*

(AC) *Всякий непостоянный многочлен кольца $K[X]$ разлагается в этом кольце в произведение многочленов первой степени.*

(AC') *Всякий непостоянный многочлен кольца $K[X]$ имеет хотя бы один корень в K.*

(AC'') *Всякий неприводимый многочлен кольца $K[X]$ является многочленом первой степени.*

(AC''') *Всякое алгебраическое расширение поля K совпадает с K* (иначе говоря, *поле K алгебраически замкнуто во всех своих надполях*).

Докажем сначала, что свойства (AC), (AC') и (AC'') эквивалентны. Ясно, что (AC) влечет (AC''); (AC'') влечет (AC'), так как всякий непостоянный многочлен кольца $K[X]$ делится на некоторый неприводимый многочлен (гл. IV, § 1, предложение 8), который, являясь многочленом первой степени, имеет корень в K. Наконец, (AC') влечет (AC), так как из (AC') индукцией по n выводится, что всякий многочлен степени n в $K[X]$ является произведением n многочленов первой степени (гл. IV, § 2, предложение 5).

Остается показать, что свойства (AC'') и (AC''') эквивалентны. Если K обладает свойством (AC''), то всякий алгебраичный над K элемент имеет степень 1 над K (§ 3, теорема 1 в)). Следовательно, он принадлежит K, т. е. выполнено условие (AC'''). Наоборот, предположим, что K обладает свойством (AC'''); пусть f — неприводимый многочлен кольца $K[X]$; тогда идеал f максимален в кольце $K[X]$, и поле $K[X]/(f)$ имеет конечную степень над K (гл. IV, § 1, предложение 4), следовательно, оно алгебраично над K (§ 3, предложение 4). Так как оно должно совпадать с K, то f имеет степень 1, и условие (AC'') доказано.

Определение 1. *Поле K называется алгебраически замкнутым, если оно обладает (эквивалентными) свойствами (AC), (AC'), (AC''), (AC''').*

Заметим, что, разумеется, поле K, *алгебраически замкнутое в данном расширении* E поля K, не обязано быть алгебраически замкнутым. Это последнее понятие имеет внутренний характер, т. е. зависит только от структуры поля K, в то время как первое существенно зависит от рассматриваемого расширения E.

Из предложения 1 вытекает следующее следствие.

Следствие. *Пусть K — подполе алгебраически замкнутого поля E; тогда алгебраическое замыкание F поля K в E является алгебраически замкнутым полем.*

Действительно, всякий непостоянный многочлен кольца $F[X]$ обладает по крайней мере одним корнем в E; этот корень, будучи алгебраичным над F, алгебраичен над K (§ 3, предложение 8), следовательно, принадлежит F.

Примеры. *1) Поле C комплексных чисел является алгебраически замкнутым (*Общ. топол.*, гл. VIII, § 1, теорема 1).

2) *Конечное* поле K не может быть алгебраически замкнутым; действительно, пусть $(x_i)_{1\leqslant i\leqslant n}$ — конечная последовательность, составленная из всех элементов поля K. Многочлен $f(X)=1+\prod_{i=1}^{n}\times$ $\times(X-x_i)$ поля $K[X]$ не может иметь корня в поле K, следовательно (предложение 1), K не является алгебраически замкнутым.

2. *Алгебраически замкнутые расширения*

Теперь мы собираемся доказать существование алгебраически замкнутого поля, содержащего произвольное данное поле. Введем следующее определение.

Определение 2. *Расширение поля K будем называть алгебраическим замыканием поля K, если оно алгебраично над K и алгебраически замкнуто.*

При доказательстве существования алгебраического замыкания мы будем пользоваться следующим важным предложением:

Предложение 2. *Пусть K — поле, $(E_\alpha)_{\alpha\in A}$ — произвольное семейство расширений поля K; тогда существует расширение E*

поля K и для каждого $\alpha \in A$ K-изоморфизм u_α расширения E_α в E такие, что E порождается объединением $u_\alpha(E_\alpha)$.

В самом деле, рассмотрим *тензорное произведение* $F = \bigotimes_{(A)} E_\alpha$ расширений E_α, рассматриваемых как алгебры над K (гл. III, приложение 1, n° 2). F — коммутативная алгебра над K, обладающая единицей, которую можно отождествить с единицей поля K, и для каждого $\alpha \in A$ существует канонический K-изоморфизм v_α расширения E_α на подполе E'_α алгебры F, содержащее K. Пусть $\mathfrak{a}$ — некоторый *максимальный идеал* алгебры F (гл. I, § 8, теорема 1); тогда факторалгебра $F/\mathfrak{a}$ является полем (гл. I, § 9, теорема 2). Так как единица расширения E'_α совпадает с единицей алгебры F, то пересечение $E_\alpha \cap \mathfrak{a}$, являющееся идеалом в E'_α, содержит лишь нуль (гл. I, § 9, предложение 2). Следовательно, канонический гомоморфизм φ алгебры F на $F/\mathfrak{a}$, ограниченный на E'_α, является K-изоморфизмом E'_α на $\varphi(E'_\alpha)$. Так как объединение расширений E'_α порождает F (гл. III, приложение 1, n° 2), то объединение полей $\varphi(E'_\alpha)$ порождает $F/\mathfrak{a}$. Таким образом, условия предложения 2 выполняются, если взять $E = F/\mathfrak{a}$ и $u_\alpha = \varphi \circ v_\alpha$ для всех $\alpha \in A$.

Чаще всего мы *будем отождествлять* E_α с $u_\alpha(E_\alpha)$ с помощью изоморфизма u_α и рассматривать поля E_α как *погруженные* в расширение E.

Теорема 1 (Штейниц). *Пусть K — поле, Ω — алгебраическое замыкание поля K, E — произвольное алгебраическое расширение поля K; тогда существует K-изоморфизм E в Ω.*

Действительно, ввиду предложения 2 существует расширение N поля K, содержащее Ω и K-изоморфизм u расширения E в N такие, что N порождается множеством $\Omega \cup u(E)$. Так как расширения Ω и $u(E)$ алгебраичны над K, то N — алгебраическое расширение поля K (§ 3, предложение 6) и тем более N алгебраично над Ω, а так как Ω — поле, алгебраически замкнутое, то $N = \Omega$ (предложение 1). Теорема доказана.

Следствие. *Пусть E и E' — два поля, u — изоморфизм E на E', F — алгебраическое расширение поля E, Ω — алгебраическое замыкание поля E'; тогда существует изоморфизм расширения F в Ω, продолжающий u.*

Пусть F' — «сумма» (Теор. мн., Рез., § 4, n° 5) множеств E' и $F \cap CE$; u_1 — взаимно однозначное отображение F на F',

продолжающее u. Перенося на F' структуру поля F с помощью отображения u_1, мы снабжаем F' структурой поля, изоморфного F, и превращаем u_1 в изоморфизм F на F', продолжающий u. Поскольку F' — алгебраическое расширение поля E', то по теореме 1 существует E'-изоморфизм v поля F' в Ω. Изоморфизм $v \circ u_1$ поля F в Ω является искомым изоморфизмом.

Возможность «продолжать» *всякое* алгебраическое расширение поля K в алгебраическое замыкание поля K *характеризует* алгебраическое замыкание поля K. Именно:

Предложение 3. *Пусть E — алгебраическое расширение поля K. Если для всякого расширения F конечной степени поля K существует K-изоморфизм F в E, то расширение E алгебраически замкнуто.*

Будем рассуждать от противного и предположим, что существует алгебраическое расширение E' поля E, отличное от E. Пусть x — элемент расширения E' и $x \notin E$. Так как x алгебраичен над E, он алгебраичен и над K (§ 3, предложение 8). Пусть f — минимальный многочлен элемента x над K, m — число *различных* корней многочлена f, *содержащихся в поле* E (m не может быть нулем), и $y_1, y_2, \ldots, y_m$ — все эти корни. Подполе $K(x, y_1, y_2, \ldots, y_m)$ является расширением поля K, содержащимся в E' и имеющим конечную степень над K (§ 3, предложение 5), и многочлен f имеет в нем не менее чем $m+1$ различных корней. Следовательно, не может существовать K-изоморфизм поля $K(x, y_1, \ldots, y_m)$ в E, так как в E многочлен f обладает только m различными корнями.

Таким образом, мы пришли к противоречию, которое доказывает предложение.

Теперь мы обладаем всем необходимым, чтобы доказать существование и единственность (с точностью до изоморфизма) алгебраического замыкания произвольного поля.

Теорема 2 (Штейниц). *Всякое поле K обладает некоторым алгебраическим замыканием. Кроме того, для любых двух алгебраических замыканий Ω и Ω' поля K существует K-изоморфизм Ω на Ω'.*

Рассмотрим алгебру многочленов $A = K[X_n]_{n \in N}$ и семейство полей $K[X_0, X_1, \ldots, X_m]/\mathfrak{a}$, где m принимает все целые положительные значения и где для каждого m, $\mathfrak{a}$ пробегает множество

всех максимальных идеалов алгебры $K[X_0, X_1, \ldots, X_m]$ *). Обозначим это семейство через $(E_\lambda)_{\lambda \in L}$. Для всякого алгебраического расширения F конечной степени поля K существует K-изоморфизм F на (по крайней мере) одно поле E_λ (§ 3, замечание 1 к предложению 5). Ввиду предложения 2 существует расширение E поля K такое, что для каждого $\lambda \in L$ существует K-изоморфизм u_λ поля E_λ в E. Пусть Ω — алгебраическое замыкание поля K в E (§ 3, n° 3); тогда Ω содержит все расширения $u_\lambda(E_\lambda)$, являющиеся алгебраическими над K. Следовательно, для всякого расширения F конечной степени поля K существует K-изоморфизм расширения F в Ω. В силу предложения 3 Ω является *алгебраическим замыканием* поля K. Если Ω' — другое алгебраическое замыкание поля K, то по теореме 1 существует K-изоморфизм v расширения Ω' в Ω, а так как поле $v(\Omega')$ алгебраически замкнуто, а Ω алгебраично над K и, следовательно, над $v(\Omega')$, то $v(\Omega') = \Omega$, чем и завершается доказательство.

Замечание. В частности, всякое *конечное* поле K допускает алгебраическое замыкание Ω, которое должно быть бесконечным полем (n° 1, пример 2). Так как всякое алгебраическое расширение конечной степени поля K является конечным полем, то Ω является алгебраическим расширением *бесконечной степени* над K.

Пусть Ω — алгебраическое замыкание поля K; тогда всякий отличный от константы многочлен f кольца $K[X]$ принадлежит кольцу $\Omega[X]$ и, следовательно (предложение 1), равен произведению множителей *первой степени* из $\Omega[X]$. Пусть x_i $(1 \leqslant i \leqslant m)$ — различные корни многочлена f в Ω; тогда сумма порядков кратности x_i *равна степени многочлена* f (см. гл. IV, § 2, теорема 2). Поле $E = K(x_1, \ldots, x_m)$, порожденное элементами x_i, называется *полем корней* (над K) многочлена f в расширении Ω. Оно алгебраично, имеет конечную степень над K (§ 3, предложение 5) и определено (независимо от Ω) с точностью до изоморфизма. Действительно, пусть F — произвольное расширение поля K такое, что многочлен f равен произведению множителей первой степени

*) Множества $K[X_0, X_1, \ldots, X_m]/\mathfrak{a}$ являются частями множества $\mathfrak{P}(A)$ (мы отождествляем $K[X_0, \ldots, X_m]$ с подалгебрами алгебры A). Укажем явно, что когда одно из этих множеств содержится в другом, мы *не предполагаем*, что первое является подполем второго (хотя можно доказать, что это действительно имеет место).

(не обязательно различных) в кольце $F[X]$. Пусть y_j $(1 \leqslant j \leqslant q)$ — различные корни многочлена f в поле F. По теореме 1 существует K-изоморфизм u подполя $K(y_1, \ldots, y_q)$ поля F на подполе E' поля Ω, а так как f равен произведению множителей первой степени в кольце $E[X]$, то элементы $x_j' = u(y_j)$ $(1 \leqslant j \leqslant q)$ являются единственными корнями многочлена f в поле Ω. Этим доказано, что $q = m$ и $x_j' = x_j$ для $1 \leqslant j \leqslant m$ (с точностью до перестановки), откуда $E' = E$. Допуская вольность речи, мы будем иногда говорить о *поле корней* многочлена f без указания расширения поля K, содержащего это поле.

Заметим, что поле корней $K(x_1, \ldots, x_m)$ многочлена f отличается, вообще говоря, от поля $K(x_i)$, порожденного *одним* из корней x_i многочлена f в Ω (см. § 6, упражнение 7). В частности, степень $K(x_1, \ldots, x_m)$ над K в общем случае *строго больше* степени многочлена f. Заметим также, что поле $K(x_1, \ldots, x_m)$, вообще говоря, не изоморфно факторкольцу $K[X]/(f)$, даже если многочлен f неприводим (если f не является неприводимым, то это факторкольцо содержит делители нуля).

Упражнения. *1) а) Пусть E — такое алгебраическое расширение поля K, что всякий многочлен, отличный от константы, кольца $K[X]$ разлагается в произведение множителей первой степени в $E[X]$. Доказать, что E является алгебраическим замыканием поля K (если элемент x алгебраичен над E, то он алгебраичен и над K; рассмотреть минимальный многочлен элемента x над K).

б) Пусть K — бесконечное поле, E — такое алгебраическое расширение поля K, что всякий многочлен, отличный от константы, кольца $K[X]$ обладает *хотя бы одним корнем* в E. Доказать, что E — алгебраическое замыкание поля K (пусть Ω — некоторое алгебраическое замыкание поля E, f — многочлен кольца $K[X]$, x_i $(1 \leqslant i \leqslant m)$ — его различные корни в Ω; рассмотреть m элементов $y_i = \sum_{j=1}^{m} z_{ij} x_j$, где z_{ij} суть m^2 произвольных элементов поля K и доказать, что можно выбрать такие z_{ij}, что $\det(z_{ij}) \neq 0$ и все y_i принадлежат полю E; использовать предложение 8 гл. IV, § 2).

2) Доказать существование алгебраического замыкания поля K, не пользуясь результатами § 4, следующим образом: рассмотреть в множестве $A = K[X] \times N$ часть $\dot{K}$, состоящую из элементов $\dot{x} = (X - x, 0)$, где x пробегает K, и перенести на $\dot{K}$ структуру поля K с помощью отображения $x \to \dot{x}$. Пусть $\mathfrak{S}$ — множество структур поля Σ, определенных на частях множества A, которое упорядочено «по продолжению», т. е. положим $\Sigma \leqslant \Sigma'$, если Σ определено

на $E \subset A$ и Σ' на $E' \subset A$ и если поле E, снабженное структурой Σ, является подполем поля E', снабженного структурой Σ'. Доказать, что $\mathfrak{S}$ — индуктивное множество; то же верно для части $\mathfrak{S}_0$ множества $\mathfrak{S}$, состоящей из структур Σ, продолжающих структуру K и таких, что для всякого элемента $z=(f(X), m)$ части множества A, на которой Σ определена, имеем $f(z)=0$ (в смысле структуры Σ). Наконец, доказать, что всякий максимальный элемент направленного множества $\mathfrak{S}_0$ является структурой алгебраически замкнутого поля, продолжающей структуру K.

3) Пусть K — поле, f — многочлен кольца $K[X, Y]$. Предположим, что имеется соотношение вида $\varphi(X) f(X, Y)=g(X, Y) h(X, Y)$, где g и h — многочлены кольца $K[X, Y]$ такие, что коэффициенты многочлена g, рассматриваемого как многочлен от Y, взаимно просты и где φ — многочлен кольца $K[X]$. Доказать, что тогда все коэффициенты многочлена h, рассматриваемого как многочлен от Y, делятся на $\varphi(X)$. (Рассмотреть φ, f, g, h как многочлены от X над полем $K(Y)$ и разложить их в произведение многочленов первой степени в алгебраическом замыкании Ω поля $K(Y)$. Заметить наконец, что если K' — алгебраическое замыкание поля K, то о. н. д. в кольце $K'[x]$ многочленов кольца $K[X]$ принадлежит $K[X]$.)

4) Пусть K — поле, u и v — рациональные дроби, отличные от констант, поля $K(X)$. Для того чтобы дробь $u(v)$ была многочленом, необходимо и достаточно, чтобы выполнялось одно из двух условий: а) либо u и v — многочлены, б) либо $u=f/(X-\alpha)^n$, $v-\alpha=\frac{1}{g}$, где f и g являются многочленами, а α — элемент поля K и степень f не превосходит n (рассмотреть алгебраическое замыкание поля K, в котором разложить на множители числитель и знаменатель рациональных дробей u и v).

§ 5. Трансцендентные расширения

1. *Алгебраически свободные семейства. Чистые расширения*

Мы собираемся обобщить определение трансцендентных элементов над полем K, данное в § 3 (определение 1).

Определение 1. *В расширении E поля K семейство $(x_\iota)_{\iota \in I}$ элементов расширения E называется алгебраически свободным над K, если идеал алгебраических соотношений между x_ι с коэффициентами в K равен* (0) (*или, что то же, если одночлены* $\prod_\iota x_\iota^{n_\iota}$ *относительно* x_ι *линейно независимы над* K).

Если семейство (x_ι) элементов расширения E не является алгебраически свободным над K, мы будем его называть алгебраически связанным над K.

Определение 1 может быть выражено еще так:

Предложение 1. *Для того чтобы семейство $(x_\iota)_{\iota\in I}$ элементов расширения E поля K было алгебраически свободным над K, необходимо и достаточно, чтобы из равенства $f((x_\iota))=0$, где f — многочлен кольца $K[X_\iota]_{\iota\in I}$, вытекало равенство $f=0$.*

Определение 2. *Расширение E поля K называется чистым расширением поля K, если существует семейство $(x_\iota)_{\iota\in I}$ элементов расширения E, алгебраически свободное над K и такое, что $E=K(x_\iota)_{\iota\in I}$. Такое семейство называется чистым базисом поля E над K.*

Пустое семейство является алгебраически свободным (гл. IV, § 1, n° 2), следовательно, K является своим собственным чистым расширением. Если множество I не пусто, и $(x_\iota)_{\iota\in I}$ — чистый базис чистого расширения E поля K, то всякий элемент этого базиса x_ι *трансцендентен* над K. В этом случае мы называем E — *чисто трансцендентным* расширением поля K. Отображение $f\to f((x_\iota))$ кольца $K[X_\iota]_{\iota\in I}$ в поле E является *изоморфизмом* этого кольца на кольцо $K[x_\iota]_{\iota\in I}$, порожденное объединением K и множества x_ι (гл. IV, § 2, теорема 1). Поле частных $E=K(x_\iota)_{\iota\in I}$ области целостности $K[x_\iota]_{\iota\in I}$, следовательно, изоморфно полю рациональных дробей $K(X_\iota)_{\iota\in I}$. Итак:

Предложение 2. *Для того чтобы расширение E поля K было чисто трансцендентным расширением поля K, необходимо и достаточно, чтобы E было изоморфно полю рациональных дробей над K. Если $(x_\iota)_{\iota\in I}$ — чистый базис расширения E, то поле E изоморфно $K(X_\iota)_{\iota\in I}$.*

Замечание. Ясно, что в произвольном расширении E поля K всякое семейство, алгебраически свободное над K, является *линейно независимым* над K. Иначе говоря, это семейство свободно для структуры *векторного пространства* расширения E (относительно K). Но обратное неверно, так как, если E — алгебраическое расширение поля K, то произвольное непустое семейство элементов из E (и тем более семейство линейно независимых элементов над K) не может быть алгебраически свободным над K. При необходимости избежать путаницы мы будем говорить, что часть расширенин E поля K, свободная для структуры векторного пространства расширения E

относительно K (соответственно базис E над K для этой структуры), является *линейно свободной* над K (соответственно *линейным базисом* E над K).

Заметим, что если семейство $(x_\iota)_{\iota\in I}$ элементов расширения E алгебраически свободно, то любые два его элемента с различными индексами различны, поскольку семейство (x_ι) линейно свободно (гл. II, § 1, n° 6).

Часть S расширения E поля K называется *алгебраически свободной частью* (или *алгебраически свободной системой*), если семейство, определяемое тождественным отображением S на себя, является алгебраически свободным (в этом случае всякое семейство, определяемое взаимно однозначным отображением множества индексов на S, является также алгебраически свободным). Элементы алгебраически свободной части расширения E называются также *алгебраически независимыми*. Если часть расширения E не является алгебраически свободной, то говорят, что она *алгебраически связана* (или является *алгебраически связанной системой*) и что ее элементы алгебраически зависимы. Если семейство элементов расширения E является чистым базисом расширения E, то множество его элементов тоже называется чистым базисом расширения E.

Всякая часть алгебраически свободной части является алгебраически свободной. Кроме того:

Предложение 3. *Для того чтобы семейство $(x_\iota)_{\iota\in I}$ элементов расширения E поля K было алгебраически свободным над K, необходимо и достаточно, чтобы всякое конечное подсемейство семейства $(x_\iota)_{\iota\in I}$ было алгебраически свободным над K.*

Предложение следует непосредственно из предложения 1.

2. Базисы трансцендентности

Предложение 4. *Пусть E — некоторое расширение поля K, M и N — части поля E. Следующие свойства эквивалентны:*

а) *множество $M \cup N$ алгебраически свободно над K и $M \cap N = \phi$,*

б) *множество M алгебраически свободно над K, а множество N алгебраически свободно над $K(M)$,*

в) *множество N алгебраически свободно над K, а множество M алгебраически свободно над $K(N)$.*

Очевидно, достаточно доказать, что а) и б) эквивалентны.

1° а) влечет б). Действительно, множество M, будучи частью объединения $M \cup N$, алгебраически свободно над полем K. Если N не является алгебраически свободным над полем $K(M)$, то существует (предложение 3) конечное семейство $(y_j)_{1 \leqslant j \leqslant n}$ различных элементов расширения N, алгебраически связанных над $K(M)$. Следовательно (гл. III, § 2, предложение 5), существует ненулевой многочлен f кольца $K[M][Y_1, \ldots, Y_n]$ такой, что $f(y_1, \ldots, y_n) = 0$. Коэффициентами многочлена f являются многочлены относительно конечного числа различных элементов $x_i (1 \leqslant i \leqslant m)$ расширения M с коэффициентами из поля K. Соотношение $f(y_1, \ldots, y_n) = 0$ можно записать в виде $g(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$, где g — ненулевой многочлен кольца $K[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$, но это соотношение противоречит предположению.

2° б) влечет а). Ясно, что $N \cap K(M) = \phi$ и тем более $M \cap N = \phi$. Достаточно доказать, что если $x_i (1 \leqslant i \leqslant m)$ — конечное число различных элементов расширения M, $y_j (1 \leqslant j \leqslant n)$ — конечное число различных элементов расширения N, то множество элементов x_i и y_j алгебраически свободно над K (предложение 3). Если это не так, то существует ненулевой многочлен $f \in K[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ такой, что $f(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$. Пусть $g = f(x_1, \ldots, x_m, Y_1, \ldots, Y_n)$ — многочлен кольца $K(M)[Y_1, \ldots, Y_n]$; тогда соотношение $f(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$ можно записать в виде $g(y_1, \ldots, y_n) = 0$. Так как множество N алгебраически свободно над полем $K(M)$, то каждый коэффициент многочлена g равен нулю, но эти коэффициенты имеют вид $\varphi(x_1, \ldots, x_m)$, где φ — многочлен кольца $K[X_1, \ldots, X_m]$. Так как эти многочлены не могут быть все равными нулю и поле M алгебраически свободно над K, мы снова приходим к противоречию.

Следствие. *Пусть E — расширение поля K, B — часть расширения E, алгебраически свободная над K. Если элемент $x \in E$ трансцендентен над $K(B)$, то множество $B \cup \{x\}$ алгебраически свободно над K.*

Предложение 5. *Пусть E — расширение поля K. Для того чтобы часть L расширения E была алгебраически свободной над K,*

необходимо и достаточно, чтобы любой элемент $x \in L$ был трансцендентным над полем $K(L \cap C\{x\})$.

Условие необходимо ввиду предложения 4. Для того чтобы доказать, что оно достаточно, предположим, что оно выполнено, и будем рассуждать от противного. Если множество L алгебраически связано над K, то существует конечная часть M множества L, алгебраически связанная над K (предложение 3). Пусть N — максимальная алгебраически свободная часть множества M и $P = M \cap CN$. По предположению, P не пусто, и всякий элемент $x \in P$ алгебраичен над полем $K(N)$ ввиду следствия из предложения 4; тем более элемент x алгебраичен над полем $K(L \cap C\{x\})$ (§ 3, предложение 2), в противоречии с предположением.

Предложение 6. *Пусть E — расширение поля K, L — часть расширения E, алгебраически свободная над K. Если $K' \subset E$ — алгебраическое расширение поля K, то множество L алгебраически свободно над K'.*

Действительно, в противном случае существовал бы (предложение 5) элемент $x \in L$, алгебраический над полем $K'(M)$, где $M = L \cap C\{x\}$. Так как $K'(M) = K(M)(K')$ и всякий элемент из K' алгебраичен над K и, следовательно, над $K(M)$ (§ 3, предложение 2), то $K'(M)$ является алгебраическим расширением поля $K(M)$ и, следовательно, x алгебраичен над $K(M)$ (§ 3, предложение 8) в противоречии с предположением.

Определение 3. *Часть B расширения E поля K называется базисом трансцендентности расширения E, если множество B алгебраически свободно над K, а поле E алгебраично над полем $K(B)$.*

Чистый базис чистого расширения поля K (определение 2) является базисом трансцендентности такого расширения. Однако необходимо заметить, что вообще трансцендентное расширение поля K не обязано быть чистым (упражнения 3 и 4).

Предложение 7. *Пусть E — расширение поля K. Всякий базис трансцендентности расширения E является максимальным элементом множества* (упорядоченного по включению) *частей расширения E, алгебраически свободных над K. Обратно, если S — часть расширения E такая, что поле E алгебраично над $K(S)$, то всякая максимальная алгебраически свободная часть множества S является базисом трансцендентности расширения E.*

Первая часть утверждения немедленно вытекает из предложения 5, поскольку, если B — базис трансцендентности расширения E над K, то всякий элемент $x \in E$ алгебраичен над полем $K(B)$. С другой стороны, если E — алгебраическое расширение поля $K(S)$, а B — максимальная алгебраически свободная часть множества S, то ввиду следствия из предложения 4 всякий элемент $x \in S$ является алгебраическим над $K(B)$. Следовательно (§ 3, предложение 8), расширение E — алгебраическое над $K(B)$.

ТЕОРЕМА 1 (Штейниц). *Всякое расширение E поля K допускает базис трансцендентности над K. Иными словами, всякое расширение поля K является алгебраическим расширением некоторого чистого расширения.*

Эта теорема является следствием следующей более точной теоремы:

ТЕОРЕМА 2. *Пусть E — расширение поля K, S — часть E такая, что поле E алгебраично над $K(S)$, L — часть множества S, алгебраически свободная над K. Тогда существует такой базис трансцендентности B расширения E над K, что $L \subset B \subset S$.*

Действительно, множество $\mathfrak{F}$ алгебраически свободных частей множества S, упорядоченное по включению, является множеством *конечного характера* (Теор. мн., Рез., § 7, n° 11) ввиду предложения 3. Следовательно, оно *индуктивно* (Теор. мн., Рез., § 7, n° 9), а тогда индуктивно и множество $\mathfrak{G}$ алгебраически свободных частей множества S, содержащих L. По теореме Цорна $\mathfrak{G}$ допускает максимальный элемент B, который является базисом трансцендентности расширения E над K ввиду предложения 7.

Заметим, что если S — *конечное* множество, то доказательство теоремы 2 проводится без использования аксиомы выбора.

СЛЕДСТВИЕ («ТЕОРЕМА ЗАМЕНЫ»). *Пусть E — расширение поля K, S — такая часть расширения E, что E алгебраично над $K(S)$, L — алгебраически свободная над K часть расширения E. Тогда существует такая часть S' множества S, что объединение $L \cup S'$ является базисом трансцендентности расширения E над K и $L \cap S' = \phi$.*

Действительно, E — алгебраическое расширение поля $K(L \cup S)$ (§ 3, предложение 2) и $L \subset L \cup S$.

Замечание. Если E — чисто трансцендентное расширение поля K, F — алгебраическое расширение поля E, отличное от E, то F вполне может быть чисто трансцендентным расширением K (см. § 3, n° 1, пример 2).

3. Степень трансцендентности расширения

Теорема 3. *Если расширение E поля K имеет конечный базис трансцендентности над K, состоящий из n элементов, то всякий другой базис трансцендентности расширения E над K состоит из n элементов.*

Достаточно доказать, что если B — базис трансцендентности поля E над K, состоящий из n элементов, то всякий другой базис трансцендентности B' расширения E над K обладает *не более чем* n элементами. Доказывать будем индукцией по n; при $n=0$ расширение E является алгебраическим над K, следовательно, всякий базис трансцендентности расширения E над K пуст по определению. Пусть x — некоторый элемент множества B'; тогда существует часть C множества B такая, что объединение $\{x\} \cup C$ составляет базис трансцендентности поля E над K и $x \notin C$ (теорема замены). Поскольку B — базис трансцендентности расширения E, то C не может совпадать с B (предложение 7), следовательно, C состоит из не более чем $n-1$ элементов. Пусть $K' = K(x)$ и $C' = B' \cap C\{x\}$, тогда множества C и C' алгебраически свободны над полем K' (предложение 4), и так как $K'(C) = K(B)$ и $K'(C') = K(B')$, то расширение E алгебраично над $K'(C)$ и $K'(C')$; иначе говоря, C и C' — два базиса трансцендентности расширения E над K'. Так как C состоит из не более чем $n-1$ элементов, то, по предположению индукции, C' тоже состоит из не более чем $n-1$ элементов, следовательно, B' состоит из не более чем n элементов.

Определение 4. *Пусть E — расширение поля K, обладающее конечным базисом трансцендентности над K. Число элементов базиса трансцендентности расширения E над K называется степенью трансцендентности или алгебраической размерностью расширения E (над K) и обозначается* $\dim \mathrm{al}_K E$ (*или* $\dim_K E$, *если не может возникнуть недоразумение*).

Смешение, которое может произойти между этим понятием и понятием *размерности* расширения E, рассматриваемого как

векторное пространство над K (т. е. (§ 2) *степенью* E над K), можно избежать, если помнить, что когда E имеет конечную и отличную от нуля алгебраическую размерность над полем K, тогда оно имеет *бесконечную* размерность над K как векторное пространство (§ 3, предложение 4).

Расширение E поля K, которое обладает бесконечным базисом трансцендентности над K, не может обладать другим конечным базисом трансцендентности над K (теорема 3); о таком расширении говорят, что оно имеет *бесконечную степень трансцендентности* (или *бесконечную алгебраическую размерность*) над K.

Когда говорят, что расширение поля K имеет алгебраическую размерность $\geqslant n$ над K, это значит, что оно имеет конечную алгебраическую размерность $\geqslant n$, *или* бесконечную алгебраическую размерность.

Из теорем 2 и 3 и определения 4 вытекают следующие следствия:

Следствие 1. *В расширении E поля K алгебраической размерности n всякая система образующих состоит из не менее чем n элементов; если существует система из n образующих, то она является чистым базисом расширения E* (которое, таким образом, является *чистым расширением* поля K).

В частности, расширение *конечного типа* поля K (§ 2, определение 1) имеет *конечную* алгебраическую размерность над K. Обратное не верно, как показывает алгебраическое расширение бесконечной степени.

Следствие 2. *В расширении E поля K, алгебраической размерности n, всякая часть, алгебраически свободная над K, имеет не более чем n элементов; алгебраически свободная часть, состоящая из n элементов, является базисом трансцендентности расширения E над K.*

Замечания. 1) Теорема 3 утверждает, что два базиса трансцендентности одного и того же расширения E поля K являются *равномощными*, если один из них конечен; в действительности утверждение верно и без этого ограничения (см. упражнение 1).

2) Читатель уже заметил аналогию между свойствами алгебраически свободных частей (соответственно базисов трансцендентности) некоторого расширения и свойствами свободных частей (соответственно базисов) векторных пространств, доказанных в гл. II, § 3.

Мы подчеркивали эту аналогию, копируя там, где было возможно, одно изложение с другого. Впрочем, оба изложения можно вывести из одной общей теории (упражнение 14).

Теорема 4. *Пусть E — расширение поля K, F — расширение E. Если одно из чисел $\dim_K F$, $\dim_K E + \dim_E F$ определено, то определено и другое, и*

$$\dim_K F = \dim_K E + \dim_E F. \tag{1}$$

Ввиду определения 4 эта теорема вытекает из следующего более общего предложения:

Предложение 8. *Пусть E — расширение поля K, F — расширение E. Если M — базис трансцендентности расширения E над K, N — базис трансцендентности расширения F над E, то пересечение $M \cap N$ — пусто, а объединение $M \cup N$ составляет базис трансцендентности поля F над K.*

Действительно, поле $E(N)$ алгебраично над $K(M \cup N) = K(M)(N)$, так как $E(N) = K(M \cup N)(E)$, и всякий элемент расширения E алгебраичен над $K(M)$, следовательно, и над $K(M \cup N)$ (§ 3, предложение 2). Тем самым (§ 3, предложение 8) поле F алгебраично над $K(M \cup N)$. С другой стороны, множество N, будучи алгебраически свободным над E, тем более алгебраически свободно над $K(M)$, следовательно (предложение 4) множество $M \cup N$ алгебраически свободно над K и $M \cap N = \phi$.

4. *Алгебраически разделенные расширения*

Определение 5. *Пусть Ω — расширение поля K, E и F — подрасширения расширения Ω. Подрасширения E и F называются алгебраически разделенными (над K), если, каковы бы ни были части A расширения E и B расширения F, алгебраически свободные над K, пересечение $A \cap B$ пусто, а объединение $A \cup B$ алгебраически свободно над K.*

Замечания. 1) Ввиду предложения 3 достаточно, чтобы условие определения 5 выполнялось для *конечных* и алгебраически свободных над K частей A и B; расширения E и F будут тогда алгебраически разделенными. Иначе говоря, достаточно, чтобы всякая пара расширений *конечного типа* E' и F' поля K, содержащихся соответственно в E и F, была алгебраически разделена. Выражаясь образно, можно сказать, что алгебраическая разделенность является свойством «конечного характера».

2) **Понятие алгебраически разделенных расширений существенно зависит от поля K: два расширения E и F поля K, алгебраически разделенные над K, не обязаны быть алгебраически разделенными над подполем K_0 поля K.**

3) **Ясно, что если расширения E и F алгебраически разделены над K, когда их рассматривают как подрасширения Ω, то они алгебраически разделены, когда их рассматривают как подрасширения поля $K(E \cup F)$, и обратно.**

Из определения 5 вытекает, что если по крайней мере одно из расширений E и F *алгебраическое* над K, то E и F *алгебраически разделены* над K. В частности, всякое алгебраическое расширение поля K является алгебраически разделенным с самим собой.

Определение 5 показывает, что если расширения E и F алгебраически разделены над K, то поле $E \cap F$ *алгебраично* над K, так как если элемент $x \in E \cap F$ является трансцендентным над K, то множество $\{x\}$ оставляет непустую часть расширений E и F, алгебраически свободную над K, что противоречит определению 5.

Предложение 9. *Пусть Ω — расширение поля K, E и F — подрасширения Ω. Если поля E и F алгебраически разделены над K, то всякая часть M* (соответственно N) *расширения E* (соответственно F), *алгебраически свободная над K, является алгебраически свободной над F* (соответственно E). *Обратно, если существует базис трансцендентности A расширения E, алгебраически свободный над F, то расширения E и F алгебраически разделены над K.*

Действительно, предположим, что поля E и F алгебраически разделены над K и B — некоторый базис трансцендентности расширения F. Ввиду определения 5 и предложения 4 множество M алгебраически свободно над $K(B)$, следовательно, и над F, так как поле F алгебраично над $K(B)$ (предложение 6). Для того чтобы доказать вторую часть предложения, заметим, что если N — часть расширения F, алгебраически свободная над K, то множество A алгебраически свободно над полем $K(N)$, следовательно (предложение 4), множество N алгебраически свободно над полем $K(A)$ (предложение 6). Наконец, если M — часть расширения E, алгебраически свободная над K, то множество N алгебраически свободно над полем $K(M)$, следовательно (предложение 4), $M \cap N = \phi$ и множество $M \cup N$ алгебраически свободно над K.

Следствие 1. *Пусть E и F — подрасширения расширения Ω, A — базис трансцендентности E над K, B — базис трансцендентности F над K; тогда поле $K(E \cup F)$ алгебраично над $K(A \cup B)$. Для того чтобы поля E и F были алгебраически разделены над K, необходимо и достаточно, чтобы пересечение $A \cap B$ было пустым, а объединение $A \cup B$ — алгебраически свободным над K; тогда множество $A \cup B$ образует базис трансцендентности расширения $K(E \cup F)$ над K.*

Поскольку $K(E \cup F) = K(A \cup B)(E \cup F)$, а всякий элемент расширения E (соответственно F) алгебраичен над $K(A)$ (соответственно $K(B)$) и тем более над $K(A \cup B)$ (§ 3, предложение 2), то расширение $K(E \cup F)$ алгебраично над $K(A \cup B)$ (§ 3, предложение 6). Если множество $A \cap B$ пусто, а $A \cup B$ алгебраически свободно над K, то A алгебраически свободно над полем $K(B)$ (предложение 4), следовательно, и над полем F, которое алгебраично над $K(B)$ (предложение 6); поэтому поля E и F алгебраически разделены над K ввиду предложения 9.

Следствие 2. *Если поля E и F алгебраически разделены над K, то алгебраические замыкания E' и F' расширений E и F в поле Ω* (§ 3, п° 3) *алгебраически разделены над K.*

Действительно, всякий базис трансцендентности расширения E (соответственно F) над K является базисом трансцендентности расширения E' (соответственно F') над K.

Предложение 10. *Пусть Ω — расширение поля K, E и F — подрасширения Ω.*

а) *Если алгебраическая размерность поля F над K конечна, то $\dim_E E(F) \leqslant \dim_K F$. Для того чтобы поля E и F были алгебраически разделены над K, необходимо и достаточно, чтобы $\dim_E E(F) = \dim_K F$.*

б) *Если, кроме того, алгебраическая размерность E над K конечна, то $\dim_K K(E \cup F) \leqslant \dim_K E + \dim_K F$. Для того чтобы поля E и F были алгебраически разделены над K, необходимо и достаточно, чтобы*

$$\dim_K K(E \cup F) = \dim_K E + \dim_K F.$$

Действительно, пусть B — некоторый базис трансцендентности поля F над K. Тогда всякий элемент поля F алгебраичен над

полем $K(B)$ и, следовательно, над полем $E(B)$. Таким образом, расширение $E(F)$ алгебраично над полем $E(B)$ (§ 3, предложение 8); отсюда следует (теорема 2), что B содержит базис трансцендентности поля $E(F)$ над E. Кроме того, если множество B составляет базис трансцендентности расширения $E(F)$ над E, то поля E и F алгебраически разделены над K, и обратно (предложение 9), что доказывает а). Утверждение б) является непосредственно вытекающим из следствия 1 предложения 9.

Читатель заметит аналогию между этим предложением и предложением 4 § 2 относительно линейно разделенных расширений (см. упражнение 14).

Понятие алгебраически разделенного расширения можно связать с понятием линейно разделенного расширения (§ 2, n° 3). Действительно, пусть расширения E и F алгебраически разделены над K, и пусть A (соответственно B) — базис трансцендентности расширения E (соответственно F) над K. Тогда определения 1 и 5 показывают, что алгебры $K[A]$ и $K[B]$ *линейно разделены* над K, и обратно, ввиду следствия 1 из предложения 9. Это равносильно (§ 2, предложение 5) утверждению, что чистые расширения $K(A)$ и $K(B)$ линейно разделены над K.

Из приведенных рассуждений легко выводится, что линейно разделенные расширения E и F поля K тем более алгебраически разделены, однако обратное не верно, как показывает пример двух алгебраических расширений, совпадающих с K. Однако имеет место следующий результат:

Предложение 11. *Пусть* Ω — *расширение поля* K, E *и* F — *подрасширения расширения* Ω, *алгебраически разделенные над* K. *Если* E — *чистое расширение поля* K, *то поля* E *и* F *линейно разделены над* K.

Действительно, пусть B — чистый базис расширения E. Так как E — поле частных кольца $K[B]$, достаточно доказать, что кольца F и $K[B]$ линейно разделены над K (§ 2, предложение 5). Множество B алгебраически свободно над F (предложение 9), следовательно, одночлены относительно элементов из B линейно независимы над F. Так как эти одночлены образуют базис (линейный) кольца $K[B]$ над полем K, то кольца $K[B]$ и F линейно разделены над K (§ 2, n° 3).

Следствие. *Всякое чистое расширение поля K линейно разделено со всяким алгебраическим расширением поля K и, в частности, не содержит алгебраических над K элементов и не совпадает с K.*

Иначе говоря, поле K алгебраически замкнуто во всяком своем чистом расширении.

Упражнения. 1) Пусть E — расширение поля K, B — бесконечный базис трансцендентности расширения E над K. Доказать, что всякая часть C расширения E такая, что E алгебраично над $K(C)$, имеет мощность не меньшую, чем мощность базиса B (для каждого элемента $x \in C$ рассмотреть его минимальный многочлен над $K(B)$ и наименьшую конечную часть F_x базиса B такую, что коэффициенты этого многочлена принадлежат $K(F_x)$; доказать, что B является объединением частей F_x). Вывести отсюда, что два произвольных базиса трансцендентности расширения E поля K равномощны. Мощность базиса называется также *степенью трансцендентности* (или *алгебраической размерностью*) расширения E поля K.

2) Пусть E — расширение поля K, B — базис трансцендентности E над K. Доказать, что множество E равномощно $K \times B$, если хотя бы одно из множеств K, B бесконечно и счетно в противном случае (см. § 3, упражнение 1 и гл. II, § 1, упражнение 14). °Вывести отсюда, в частности, что всякий базис трансцендентности поля R действительных чисел над полем Q рациональных чисел имеет мощность континуума.°

3) Пусть K — поле $Q(X)$ рациональных дробей от одной переменной X над полем Q рациональных чисел. Доказать, что в кольце $K[Y]$ многочлен Y^2+X^2+1 неприводим и что если E — расширение поля K, порожденное корнем этого многочлена (в алгебраическом замыкании поля K), то всякий элемент расширения E, не принадлежащий Q, трансцендентен над Q, но E не является чистым расширением Q (чтобы доказать отсутствие в E элементов, алгебраических над Q, заметить, что ввиду предложения 11 $E = Q(a)(X)$, $a \notin Q$, $a \in E$, и обратить внимание на то, что элемент $-(X^2+1)$ не является квадратом в поле $A(X)$, где A — алгебраическое замыкание поля Q). Доказать, что если i — корень многочлена x^2+1, то $E(i)$ — чисто трансцендентное расширение поля $Q(i)$ («параметрическое представление кривой второго порядка»).

*°4) Пусть K — поле $C(X)$ рациональных дробей от одной переменной X над полем (алгебраически замкнутым) C комплексных чисел. Доказать, что в кольце $K[Y]$ многочлен Y^3+X^3+1 неприводим. Пусть E — расширение поля K, порожденное корнем этого многочлена (в алгебраическом замыкании поля K). Доказать, что всякий элемент расширения E, не принадлежащий C, трансцендентен

над C, но что E не является чистым расширением C (чтобы установить это, доказать невозможность равенства $u^3+v^3+w^3=0$, где попарно простые и не все постоянные u, v, w — многочлены кольца $C[X]$. Для этого рассуждаем от противного. Если r — наибольшая из степеней многочленов u, v, w и, скажем, $\deg w=r$, то из соотношения

$$w^3=-(u+v)(u+jv)(u+j^2v),$$

где j и j^2 — корни третьей степени из единицы, вывести, что существуют три многочлена u_1, v_1, w_1 попарно простые и не все постоянные, имеющие степени меньше r и такие, что $u_1^3+v_1^3+w_1^3=0$).

*5) Пусть E — трансцендентное расширение поля k, x — трансцендентный над K элемент поля E; всякий элемент $y\in K(x)$ можно записать в виде $f(x)=g(x)/h(x)$, где g и h — взаимно простые многочлены кольца $K[X]$, однозначно определенные с точностью до множителя из полн K. Назовем *высотой* элемента y относительно x наибольшую из степеней многочленов g и h.

а) Доказать, что в кольце $K(y)[X]$ многочлен $g(X)-yh(X)$ неприводим (использовать упражнение 3 из § 4). Вывести отсюда, что если элемент y имеет высоту n относительно x, то поле $K(x)$ является алгебраическим расширением степени n поля $K(y)$.

б) Вывести из а), что всякий элемент $y\in K(x)$, для которого $K(y)=K(x)$, имеет вид $(ax+b)/(cx+d)$, где a, b, c, d — элементы поля K, подчиненные условию $ad-bc\neq 0$; доказать обратное утверждение. Найти все K — автоморфизмы поля $K(x)$.

в) Доказать, что если элемент $y\in K(x)$ имеет высоту n относительно x, а элемент $z\in K(y)$ имеет высоту m относительно y, то элемент z имеет высоту mn относительно x.

г) Пусть F — такое расширение поля K, что $K\subset F\subset K(x)$ и $F\neq K$; пусть y — элемент расширенин F, высота которого m относительно x принимает наименьшее возможное значение; доказать, что $F=K(y)$ («теорема Люрота»). (Пусть φ — минимальный многочлен элемента x над полем F; доказать, что $\varphi=u(X, y)/w(y)$, где u — многочлен кольца $K[X, Y]$ степени не меньше m относительно Y и не делящийся ни на какой непостоянный многочлен кольца $K[Y]$; если $y=g(x)/h(x)$, где g и h взаимно просты, заметить, что вриду а) многочлен $g(X)h(Y)-g(Y)h(X)$ не делится ни на какой непостоянный многочлен кольца $K[X]$ или $K[Y]$; вывести отсюда, что

$$g(X)h(Y)-g(Y)h(X)=Ku(X, Y),$$

используя упражнение 3 § 4).

6) Вывести из упражнения 5 в) другое доказательство упражнения 4 § 4 (заметить, что в случае, когда степень v больше нуля, степень многочлена $u(v)$ равна его высоте).

7) Пусть F — расширение конечного типа поля K. Доказать, что всякое поле E, промежуточное между K и F, является расширением

конечного типа поля K (пусть B — базис трансцендентности расширения E поля K, C — базис трансцендентности поля F над E; доказать, что E имеет конечную степень над $K(B)$, используя, что F имеет конечную степень над $K(B \cup C)$ и что расширение E и $K(B \cup C)$ линейно разделены над $K(B)$ (предложение 11).

*8) Пусть Ω — расширение поля K, E и F — расширения поля K, содержащиеся в Ω и алгебраически разделенные над K. Доказать, что для того, чтобы E и F были линейно разделены над K, необходимо и достаточно, чтобы тензорное произведение $E \otimes F$ (относительно K) было областью целостности (чтобы доказать достаточность, рассмотреть базис трансцендентности A расширения E над K и базис трансцендентности B расширения F над K. Доказать, что поле частных H кольца $E \otimes F$ алгебраично над полем частных L кольца $K(A) \otimes K(B)$. Пусть φ — канонический изоморфизм кольца $E \otimes F$ в поле $K(E \cup F)$, z некоторый элемент кольца $E \otimes F$, $\sum_{i=0}^{n} v_i X^{n-i}$ — минимальный многочлен элемента z над L, умноженный на некоторый ненулевой элемент кольца $K(A) \otimes K(B)$, так, что коэффициенты v_i принадлежат кольцу $K(A) \otimes K(B)$. Доказать, что равенство $\varphi(z)=0$ влечет $\varphi(v_n)=0$ и, следовательно, $z=0$).

9) Пусть Ω — расширение поля K, E и F — подрасширения Ω, линейно разделенные над K. Пусть σ и τ — K-изоморфизмы полей E и F соответственно в поле Ω. Доказать, что если поля $\sigma(E)$ и $\tau(F)$ алгебраически разделены над K, то они линейно разделены над K и существует единственный K-изоморфизм θ расширения $K(E \cup F)$ на $K(\sigma(E) \cup \tau(F))$, который совпадает с σ на E и τ на F.

10) В алгебраическом замыкании Ω поля $Q(X)$ рассматриваются два чисто трансцендентных расширения $E=Q(X)$ и $F=Q(X+i)$ (где $i^2=-1$) поля Q. Доказать, что E и F не являются алгебраически разделенными над Q, но $E \cap F=Q$ (пусть p и q — взаимно простые многочлены кольца $Q[X]$, а также r и s взаимно просты в $Q[X]$; доказать невозможность равенства $p(X+i)s(X) = q(X+i)r(X)$, заметив, что взаимно простые многочлены в кольце $Q[X]$ остаются взаимно простыми в кольце $\Omega[X]$).

11) Пусть E, F, G — расширения поля K, содержащиеся в расширении Ω поля K, и пусть $F \subset G$. Для того чтобы поля E и G были алгебраически разделены над K, необходимо и достаточно, чтобы поля E и F были алгебраически разделены над K и чтобы поля $E(F)$ и G были алгебраически разделены над F.

*12) а) Пусть K — поле, L — подполе поля K; предположим, что существует конечное число элементов a_i $(1 \leqslant i \leqslant n)$ поля K таких, что $K=L[a_1, a_2, \ldots, a_n]$. Доказать, что элементы a_i *алгебраичны* над L (рассуждая от противного, предположить, что $a_1, \ldots, a_m$ $(m \geqslant 1)$ образуют максимальное алгебраически свободное подсемейство семейства $(a_i)_{1 \leqslant i \leqslant n}$, заметить, что в кольце $A=L[a_1, \ldots, a_m]$ пересечение

всех максимальных идеалов равно (0), применить упражнение 4б), из § 3).

б) Вывести из а), что в алгебре многочленов $K[X_1, \ldots, X_n]$ всякий максимальный идеал имеет *конечную* коразмерность над K. Вывести отсюда, что если A—коммутативная алгебра над полем K, обладающая единицей и если существует конечное число элементов $b_j \in A$ $(1 \leqslant j \leqslant q)$ таких, что $A = K[b_1, b_2, \ldots, b_q]$, то всякое подполе алгебры A, содержащее K, имеет конечный ранг над K.

13) Пусть K—поле, $K((X))$—поле формальных рядов от одной переменной над K (гл. IV, § 5, n° 7). Доказать, что всякий базис трансцендентности поля $K((X))$ над K равномощен множеству K^N. Будем различать два случая:

а) Если мощность множества K строго меньше мощности K^N, то заметить, что множество $K((X))$ равномощно K^N, и использовать упражнение 2.

б) Если множества K и K^N равномощны, то пусть P—простое подполе поля K, S—некоторое бесконечное множество элементов поля $K((X))$, алгебраически независимых над K, T—множество (равномощное S) коэффициентов всех формальных рядов, принадлежащих S. Пусть L—алгебраическое замыкание в $K((X))$ поля $K(S)$; пусть u—элемент поля L и f—его минимальный многочлен над $K(S)$. Умножая f на ненулевой элемент поля $K(S)$, можно считать, что u удовлетворяет уравнению вида $g(s_1, \ldots, s_m, u) = 0$, где g—многочлен кольца $K[X_1, \ldots, X_m, X_{m+1}]$, а $s_1, \ldots, s_m$—элементы множества S. Пусть A—множество коэффициентов многочлена g, $C(u)$—множество коэффициентов формального ряда u. Доказать, что поле $P(T)(A \cup C(u))$ алгебраично над $P(T \cup A)$, показать, что в противном случае должно существовать бесконечное множество степенных рядов v, принадлежащих полю $\Omega((X))$, где Ω—алгебраическое замыкание поля K, удовлетворяющих уравнению $g(s_1, \ldots, s_m, v) = 0$. Используя упражнение 2, доказать, что если множество S имеет строго меньшую мощность, чем мощность K, то степень трансцендентности поля K над $P(T)$ бесконечна, и вывести отсюда, что в этом случае поле L отлично от $K((X))$.

*14). Пусть E—некоторое множество, φ—отображение множества $\mathfrak{P}(E)$ в $\mathfrak{P}(E)$, удовлетворяющее следующим условиям: 1° $X \subset \varphi(X)$ для всех $X \subset E$; 2° $\varphi(\varphi(X)) = \varphi(X)$ для всех $X \subset E$; 3° для всякого $X \subset E$ $\varphi(X)$ является объединением множеств $\varphi(Y)$, где Y пробегает множество конечных частей X; 4° если $y \notin \varphi(X)$ и $y \in \varphi(X \cup \{x\})$, то $x \in \varphi(X \cup \{y\})$ («аксиома замены»). Часть X множества E назовем *системой* φ-*образующих* части Z, если $Z = \varphi(X)$. Назовем X φ-*свободной* частью множества E, если X—*минимальная* система φ-образующих $\varphi(X)$. Назовем φ-*базисом* множества Z систему φ-образующих этого множества, являющуюся φ-свободной.

а) Доказать, что если множество X φ-свободно и $x \notin \varphi(X)$, то множество $X \cup \{x\}$ φ-свободно Вывести отсюда, что всякая

максимальная φ-свободная часть части Y множества E является φ-базисом множества $\varphi(Y)$.

б) Пусть A — некоторая часть множества E, Y — система φ-образующих множества A, X — φ-свободная часть Y. Доказать существование такого φ-базиса B части A, что $X \subset B \subset Y$.

в) Если A — произвольная часть множества E, то отображение φ_A $\mathfrak{P}(E)$ в $\mathfrak{P}(E)$, определяемое соотношением $\varphi_A(X) = \varphi(A \cup X)$, удовлетворяет тем же уравнениям, что и φ.

г) Если A — часть множества E, обладающая φ-базисом из n элементов, то всякий другой φ-базис части A состоит из n элементов (рассуждать индукцией по n: пусть B есть φ-базис из n элементов части A, B' — другой φ-базис; рассмотреть элемент $a \in B'$. Доказать, с помощью б) существование части C базиса B такой, что $\{a\} \cup C$ — φ-базис части A и $a \notin C$; наконец, применить предположение индукции к функции $\varphi_{\{a\}}$).

д) Две части A и B множества E назовем φ-разделенными, если пересечение всякой φ-свободной части множества A с φ-свободной частью множества B пусто и если объединение всякой φ-свободной части множества A и всякой φ-свободной части множества B φ-свободно. Доказать, что для того, чтобы части A и B были φ-разделены, необходимо и достаточно, чтобы всякая φ-свободная часть A была φ_B-свободной.

§ 6. Продолжения изоморфизмов. Сопряженные элементы Нормальные расширения.

1. *Продолжения изоморфизмов*

Теорема 1 § 4, устанавливающая возможность «погрузить» всякое алгебраическое расширение поля K в алгебраическое замыкание поля K, следующим образом обобщается на трансцендентные расширения.

Предложение 1. *Пусть E — расширение поля K, $(a_\iota)_{\iota \in I}$ — базис трансцендентности расширения E над K. Пусть K' — поле, изоморфное полю K, и Ω — алгебраически замкнутое расширение поля K'. Для всякого изоморфизма u_0 поля K на K' и всякого семейства $(b_\iota)_{\iota \in I}$ элементов расширения Ω, алгебраически свободного над K' и имеющего то же множество индексов, что (a_ι), существует изоморфизм u расширения E в Ω, продолжающий u_0 и такой, что $u(a_\iota) = b_\iota$ для всех $\iota \in I$.*

Действительно, существует изоморфизм $f \to \bar{f}$ поля $K(X_\iota)_{\iota \in I}$ на $K'(X_\iota)_{\iota \in I}$, который продолжает u_0 и оставляет инвариантными

переменные X_ι (гл. IV, § 3, предложение 1). Следовательно, определен изоморфизм u_1 чистого расширения $K(a_\iota)_{\iota\in I}$ на чистое расширение $K'(b_\iota)_{\iota\in I}$, продолжающий u_0 и ставящий в соответствие каждому элементу $f((a_\iota))$ (где $f\in K(X_\iota)_{\iota\in I}$) элемент $\overline{f}((b_\iota))$ (§ 5, предложение 2). Пусть F — алгебраическое замыкание поля $K'(b_\iota)_{\iota\in I}$ в Ω; тогда поле F алгебраически замкнуто (§ 4, следствие из предложения 1), следовательно, поскольку расширение E алгебраично над $K(a_\iota)_{\iota\in I}$, существует изоморфизм u расширения E на F, продолжающий u_1 (§ 4, следствие из теоремы 1).

Заметим, что существование семейства $(b_\iota)_{\iota\in I}$ элементов расширения Ω, алгебраически свободного над K', обеспечивается, в частности, когда $K'=K$ и алгебраическая размерность E *конечна* и не превосходит алгебраической размерности Ω (над K). Всякое расширение поля K, имеющее конечную алгебраическую размерность над K, может быть, таким образом, погружено, например, в *единственное* алгебраическое замыкание Ω_0 расширения $K(X_n)_{n\in N}$ поля K. Такое расширение называется *универсальным расширением* для расширений поля K конечной алгебраической размерности.

Следствие. *Пусть Ω — алгебраически замкнутое расширение поля K бесконечной алгебраической размерности над K. Пусть E_i $(1\leqslant i\leqslant n)$ — n расширений поля K конечной алгебраической размерности над K. Можно найти для каждого индекса i $(1\leqslant i\leqslant n)$ такой K-изоморфизм u_i расширения E_i в Ω, что поле $u_i(E_i)$ будет алгебраически разделено (над K) с подполем расширения Ω, порожденным $n-1$ подполем $u_j(E_j)$ с индексами $j\neq i$.*

Действительно, пусть B — базис трансцендентности (бесконечный) расширения Ω над полем K. Для каждого индекса i определим множество B_i как часть базиса B, состоящего из такого числа элементов, какова алгебраическая размерность поля E_i над K; выберем B_i так, чтобы они попарно не пересекались. Ввиду предложения 1 существует K-изоморфизм u_i расширения E_i в Ω такой, что B_i — базис трансцендентности поля $u_i(E_i)$ над K. Следствие вытекает теперь из § 5, следствия 1 из предложения 9.

Предложение 2. *Пусть Ω — алгебраически замкнутое расширение поля K, E — подрасширение Ω, u — некоторый K-изоморфизм E в Ω. Если существуют два равномощных базиса транс-*

цендентности расширения Ω *над* E *и над* $u(E)$ *соответственно, то и продолжается до* K*-автоморфизма поля* Ω.

Действительно, пусть B — базис трансцендентности поля Ω над E, C — базис трансцендентности поля Ω над $F=u(E)$, равномощный B. Ввиду предложения 1 существует изоморфизм v поля $E(B)$ на $F(C)$, продолжающий u. Так как Ω — алгебраическое замыкание полей $E(B)$ и $F(C)$, то (§ 4, следствие из теоремы 1) существует изоморфизм w расширения Ω в себя, продолжающий v. Поскольку $w(\Omega)$ — алгебраическое замыкание поля $F(C)$, содержащееся в Ω, то $w(\Omega)=\Omega$; это показывает, что w — K-автоморфизм поля Ω.

Следствие 1. *Пусть* Ω *— алгебраически замкнутое расширение поля* K, E *— подрасширение* Ω. *Всякий* K*-автоморфизм поля* E *продолжается до* K*-автоморфизма поля* Ω.

Следствие 2. *Пусть* Ω *— алгебраически замкнутое расширение поля* K, E *— подрасширение* Ω *конечной алгебраической размерности над* K; *тогда всякий* K*-изоморфизм и расширения* E *в* Ω *продолжается до* K*-автоморфизма поля* Ω.

Действительно, пусть n — алгебраическая размерность поля E над K; она совпадает с алгебраической размерностью поля $u(E)=F$ над K. Следовательно, поле $G=K(E\bigcup F)$ имеет конечную алгебраическую размерность $m\leqslant 2n$ над K (§ 5, предложение 10). Поле G имеет одинаковую алгебраическую размерность $m-n$ над E и над F (§ 5, теорема 4). Пусть A — базис трансцендентности поля G над E, а B — базис трансцендентности поля G над F. Для всякого базиса трансцендентности C поля Ω над G множества $A\bigcup C$ и $B\bigcup C$ будут базисами трансцендентности поля Ω над E и F соответственно (§ 5, предложение 8), притом равномощными, так как базисы A и B равномощны. Следствие вытекает теперь из предложения 2.

Это следствие перестает быть верным в случае *произвольного* подрасширения E расширения Ω (упражнение 2).

2. *Сопряженные поля. Сопряженные элементы*

Определение 1. *Пусть* Ω *— алгебраически замкнутое расширение поля* K, E *и* F *— подрасширения расширения* Ω. *Подрасширения* E *и* F *называются сопряженными (над* K*) в поле* Ω, *если существует такой* K*-автоморфизм и расширения* Ω, *что*

$u(E)=F$. *Два элемента x и y расширения Ω называются сопряженными над K, если существует такой K-автоморфизм и расширения Ω, что $u(x)=y$.*

Пусть u — некоторый K-автоморфизм поля Ω, A — произвольная часть Ω и $E=K(A)$; тогда значения u в E полностью определяются значениями u в A и $u(E)=K(u(A))$ (гл. IV, § 3, следствие из предложения 2). В частности, если x и y — элементы поля Ω, сопряженные над K, то $K(x)$ и $K(y)$ — расширения поля K, сопряженные в Ω.

Разумеется, значения, которые может принимать K-автоморфизм u расширения Ω для элементов части A поля E, не являются в общем случае произвольными (см. предложение 3). Заметим, что отношение «x и y сопряжены» является отношением эквивалентности в Ω, классы, соответствующие этому отношению, являются *классами интранзитивности* группы K-автоморфизмов расширения Ω (гл. I, § 7, n° 5).

Предложение 3. *Для того чтобы элементы x и y расширения Ω были сопряжены над K, необходимо и достаточно, чтобы либо оба они были трансцендентными над K, либо оба алгебраическими над K с одним и тем же минимальным многочленом над K.*

Условие *необходимо*, так как, если u — произвольный K-автоморфизм расширения Ω и если x — трансцендентный элемент (соответственно алгебраический) над K, то и элемент $y=u(x)$ трансцендентен (соответственно алгебраичен) над K, поскольку для любого многочлена $f\in K[X]$ выполняется тождество $u(f(x))=f(u(x))$. Это же соотношение показывает, что если элемент x алгебраичен над K и f — его минимальный многочлен над K, то $f(u(x))=0$. Следовательно, поскольку многочлен f неприводим в кольце $K[X]$, то он является минимальным для элемента $y=u(x)$ (§ 3, определение 1).

Условие *достаточно*. Предположим сначала, что элементы x и y — трансцендентны над K (а в остальном произвольные). Поскольку отображение $f\to f(x)$ (соответственно $f\to f(y)$) поля $K(X)$ на $K(x)$ (соответственно на $K(y)$) является K-изоморфизмом, существует K-изоморфизм u расширения $K(x)$ на $K(y)$ такой, что $u(x)=y$ и этот K-изоморфизм продолжается до некоторого K-автоморфизма поля Ω (следствие 2 из предложения 2). Следовательно, элементы x и y сопряжены над K.

Если же элементы x и y алгебраичны над K и имеют один и тот же минимальный многочлен f, то существует некоторый K-изоморфизм поля $K[X]/(f)$ на $K(x)$ (соответственно на $K(y)$), переводящий класс X по модулю (f) в элемент x (соответственно в y) (§ 3, теорема 1); следовательно, существует K-изоморфизм u расширения $K(x)$ на $K(y)$ такой, что $u(x)=y$. Окончание рассуждения проводится, как выше.

Этот результат показывает, что понятие сопряженных элементов *в данном расширении* E поля K является *внутренним*, т. е. зависит только от структуры расширения E, но не от алгебраически замкнутого поля Ω, в которое вкладывается E.

Следствие. *Для того чтобы элемент $x\in\Omega$ был алгебраическим над K, необходимо и достаточно, чтобы число элементов, сопряженных с x над K, было конечным; это число не превосходит степени x над K.*

Действительно, если элемент x трансцендентен над K, то все элементы x^n (n — целое число, большее нуля) трансцендентны над K и, следовательно, сопряжены с x. С другой стороны, если элемент x алгебраичен над K, то число сопряженных с ним равно числу *различных* корней в поле Ω его минимального многочлена f (над K), т. е. не превосходит степени многочлена f (гл. IV, § 2, теорема 2).

Замечание. Пусть G — некоторое подрасширение расширения Ω; два элемента x и y поля G могут быть сопряжены над K, но может не существовать K-автоморфизма поля G, переводящего x в y. °Например, в поле действительных чисел R элементы $\sqrt{2}$ и $-\sqrt{2}$ сопряжены над полем Q рациональных чисел, однако не существует автоморфизмов поля R, отличных от тождественного (Общ. топол., гл. I § 3, упражнение 3).°

3. *Нормальные расширения*

Предложение 4. *Пусть E — алгебраическое расширение поля K. Тогда всякий K-эндоморфизм и расширения E является автоморфизмом поля E.*

Достаточно доказать, что $u(E)=E$. Для каждого элемента $x\in E$ обозначим символом F_x множество элементов поля E, сопряженных с x над K. Множество F_x *конечно* для любого $x\in E$, и E является объединением всех множеств F_x, когда x пробегает E.

Для каждого $y \in F_x$ элемент $u(y)$ сопряжен с y (следствие 2 из предложения 2), следовательно с x, откуда $u(F_x) \subset F_x$, а так как множество F_x конечно, то отображение u взаимно однозначно, так что $u(F_x) = F_x$, следовательно, $u(E) = E$.

Предложение 5. *Пусть Ω — алгебраически замкнутое расширение поля K, E — алгебраическое расширение K, содержащееся в Ω. Для того чтобы всякий K-изоморфизм поля E в Ω был автоморфизмом E, необходимо и достаточно, чтобы для любого $x \in E$ все элементы, сопряженные с x над K, принадлежали E.*

Так как всякий K-изоморфизм поля E в Ω продолжается до K-автоморфизма поля Ω (следствие 2 из предложения 2), это условие необходимо. Оно является достаточным, так как для каждого K-автоморфизма u расширения Ω из этого условия вытекает включение $u(E) \subset E$ (определение 1), следовательно, $u(E) = E$ (предложение 4).

Определение 2. *Алгебраическое расширение E поля K называется нормальным (над K), если всякий неприводимый многочлен кольца $K[X]$, обладающий хотя бы одним корнем в E, разлагается в произведение множителей первой степени* (не обязательно различных) *в кольце $E[X]$.*

После того как введено это определение, из характеризации сопряженных элементов (предложение 3) следует, что предложение 5 можно сформулировать в следующей эквивалентной форме:

Предложение 6. *Пусть Ω — алгебраически замкнутое расширение поля K, E — алгебраическое расширение K, содержащееся в Ω. Для того чтобы всякий K-изоморфизм поля E в Ω был автоморфизмом расширения E, необходимо и достаточно, чтобы E было нормальным над K.*

Можно сказать еще, что нормальное расширение $E \subset \Omega$ поля K характеризуется тем, что *совпадает со всеми своими сопряженными над K* (определение 1).

На протяжении всего этого n° *расширение Ω будет (произвольным) алгебраически замкнутым расширением поля K и все расширения поля K, которые мы будем рассматривать, будут подрасширениями поля Ω.*

Так как алгебраическое замыкание поля K в Ω является полем алгебраически замкнутым (§ 4, следствие из предложения 1), то оно будет нормальным расширением поля K.

Предложение 7. *Пусть N — нормальное расширение поля K, E — подрасширение N. Всякий K-изоморфизм поля E в Ω отображает E в N и может быть продолжен до K-автоморфизма поля N.*

Действительно, всякий K-изоморфизм u расширения E в Ω можно продолжить до K-автоморфизма поля Ω (следствие 2 из предложения 2), следовательно, ограничение его на поле N является K-автоморфизмом этого поля (предложение 6).

Предложение 8. *Пусть (N_ι) — некоторое семейство нормальных расширений поля K. Пересечение $\bigcap_\iota N_\iota$ и поле $K(\bigcup_\iota N_\iota)$, порожденное объединением полей N_ι, являются нормальными расширениями поля K.*

Действительно, пусть u — некоторый K-автоморфизм поля Ω. По предположению, $u(N_\iota) = N_\iota$ для всех ι, следовательно, полагая $N = \bigcap_\iota N_\iota$, имеем $u(N) = N$, т. е. расширение N нормально над K (предложение 6). Аналогично, пусть $M = K(\bigcup_\iota N_\iota)$; тогда $u(M)$ порождается объединением полей $u(N_\iota) = N_\iota$, следовательно, совпадает с M, так что M нормально над K.

Из предложения 8, в частности, следует, что для *произвольного* алгебраического расширения E поля K существует *наименьшее нормальное расширение* N поля K, содержащее E, а именно пересечение всех нормальных расширений поля K, содержащих E (они заведомо существуют, например, алгебраическое замыкание поля K в Ω). Будем называть N нормальным расширением, *порожденным расширением* E.

Предложение 9. *Пусть A — некоторое множество алгебраических над K элементов расширения Ω, и пусть B — множество сопряженных (над K) с элементами A элементов множества Ω. Тогда поле $K(B)$ является нормальным расширением поля K, порожденным $K(A)$.*

Действительно, всякое нормальное расширение поля K, содержащее A, должно содержать B (предложение 5); кроме того, расширение $K(B)$ нормально над K, так как для любого K-автоморфизма u расширения Ω, имеет место включение $u(B) \subset B$ (определение 1), следовательно, $u(K(B)) = K(u(B)) \subset K(B)$.

Следствие 1. *Пусть E — алгебраическое расширение поля K конечной степени; тогда нормальное расширение N поля K, порожденное E, тоже имеет конечную степень.*

Действительно, $E=K(A)$, где A—некоторое конечное множество (§ 2, n° 2), следовательно, множество B элементов, сопряженных с элементами A, конечно, и следствие доказано (§ 3, предложение 5).

Следствие 2. *Всякое нормальное расширение N поля K является объединением нормальных подрасширений расширения N конечной степени над K.*

Действительно, N—объединение расширений $K(A)$, где A пробегает множество всех конечных частей расширения N (§ 2, следствие из предложения 3). Тем более N является объединением нормальных расширений, порожденных этими расширениями.

Следствие 3. *Пусть (f_ι)—некоторое семейство многочленов кольца $K[X]$, A—множество их корней в поле Ω; тогда $K(A)$—нормальное расширение поля K.*

Действительно, множество элементов, сопряженных с элементами A, совпадает с A (предложение 3).

В частности, *поле корней* (§ 4, n° 2) многочлена $f\in K[X]$ есть нормальное расширение поля K.

Мы уже отмечали (§ 4, n° 2), что поле $K(x_1, x_2, \ldots, x_n)$, порожденное корнями x_i $(1\leqslant i\leqslant n)$ многочлена f, вообще говоря, отлично от поля $K(x_i)$, порожденного только *одним* из корней (упражнение 7). Если f неприводим и $K(x_i)$ совпадает с $K(x_1, x_2, \ldots, x_n)$ для некоторого индекса i, то $K(x_j)=K(x_i)$ для всех остальных индексов j, так как поле $K(x_j)$ сопряжено с $K(x_i)$. В этом случае уравнение $f(x)=0$ называют *нормальным уравнением* над K.

Замечание. Если E—нормальное расширение поля K, а F—нормальное расширение поля E, то F *не обязательно* является нормальным расширением K. Действительно, K-автоморфизм u расширения Ω переводит в общем случае минимальный многочлен *над* E элемента $x\in F$ в *другой* многочлен кольца $E[X]$ и, следовательно, не переводит x в сопряженный с x *над* E. Таким образом, элемент $u(x)$ не обязан принадлежать полю F (упражнение 7); в этом случае F и $u(F)$—*различные* нормальные расширения поля E, которые *K-изоморфны, но не являются E-изоморфными.*

Упражнения. 1) Пусть Ω—алгебраически замкнутое расширение поля K, имеющее бесконечную алгебраическую размерность над K. Доказать существование бесконечного множества

K-эндоморфизмов Ω на подполя Ω, отличные от Ω, и по отношению к которым поле Ω имеет произвольную алгебраическую размерность, не превосходящую его размерности над K (§ 5, упражнение 1). °В частности, существует бесконечное множество различных изоморфизмов поля C комплексных чисел на подполя C, отличные от C.°

2) Пусть Ω — алгебраически замкнутое расширение поля K и E — подрасширение Ω. Доказать, что если E имеет бесконечную алгебраическую размерность над K, строго меньшую алгебраической размерности поля Ω над K (§ 5, упражнение 1), то всякий K-изоморфизм поля E в Ω можно продолжить до K-автоморфизма поля Ω. Дать пример расширения E, имеющего ту же алгебраическую размерность, что Ω, и K-изоморфизма поля E в Ω, который нельзя продолжить до K-изоморфизма (в Ω) никакого расширения поля E, содержащегося в Ω и отличного от E (см. упражнение 1).

3) Пусть Ω — алгебраически замкнутое расширение поля K конечной алгебраической размерности над K. Доказать, что всякий K-эндоморфизм поля Ω является K-автоморфизмом.

4) Пусть Ω — алгебраически замкнутое расширение поля K, E — подрасширение поля Ω, трансцендентное над K. Доказать существование бесконечного множества K-изоморфизмов поля E в Ω (пусть элемент $x \in E$ трансцендентен над K; рассмотреть подрасширение F расширения E такое, что x трансцендентен над F, а E алгебраично над $F(x)$, доказать существование бесконечного множества F-изоморфизмов поля E в Ω).

*5) Пусть Ω — алгебраически замкнутое расширение поля K, N — подрасширение поля Ω. Доказать, что если N нормально над K и если E и E' — сопряженные расширения поля K, содержащиеся в Ω, то поля $N(E)$ и $N(E')$ сопряжены над K. Обратно, если N обладает этим свойством и имеет конечную алгебраическую размерность, строго меньшую алгебраической размерности поля Ω над K, то N — нормальное алгебраическое расширение поля K.

6) Всякое алгебраическое расширение N поля K, порожденное множеством элементов, каждый из которых имеет степень 2 над K, является нормальным над K.

°7) Многочлен X^2-2 неприводим в кольце $Q[X]$. Пусть α — один из его корней. Доказать, что многочлен $X^2-\alpha$ неприводим над полем $E=Q(\alpha)$; пусть β — один из корней этого многочлена, и пусть $F=E(\beta)=Q(\beta)$. Доказать, что F не является нормальным расширением поля Q (доказать что многочлен X^2+1 неприводим над F). Каково нормальное расширение поля Q, порожденное F?°

*8) а) Доказать, что если рациональная дробь $h \in K(X)$ удовлетворяет уравнению вида $h^n+\sum f_i h^{n-i}=0$, где f_i — многочлены кольца $K[X]$, то $h \in K[X]$ (записать $h=u/v$, где u и v — взаимно простые многочлены; если v не постоянный многочлен, то рассмотреть корень v в Ω).

б) Пусть F — такое расширение поля K, что K алгебраически замкнуто в F. Доказать, что поле $K(X)$ алгебраически замкнуто в $F(X)$. (Если элемент $w \in F(X)$ алгебраичен над $K(X)$, то сначала доказать с помощью а) существование многочлена $g \in K[X]$ такого, что элемент $h = gw$ является многочленом кольца $F[X]$. Пусть $\overline{F}$ — алгебраическое замыкание поля F в Ω, и пусть $h = \sum_{j=0}^{m} a_j X^j$, где $a_j \in F$. Для каждого K-автоморфизма u расширения $\overline{F}$ доказать, что элемент $\sum_{j=0}^{m} u(a_j) X^j$ сопряжен с h над $K(X)$ и, используя предложение 3, вывести отсюда, что коэффициенты a_j принадлежат полю K.)

в) Пусть E и F — расширения поля K, алгебраически разделенные над K, и L — алгебраическое замыкание поля K в F. Вывести из б), что если E — чисто трансцендентное расширение поля K, то $E(L)$ — алгебраическое замыкание поля E в $E(F)$. (Свести к случаю, когда $K = L$ и E имеет конечную алгебраическую размерность над K (см. § 5, упражнение 10 и § 9, упражнения 2 и 3).)

§ 7. Сепарабельные расширения

1. Теорема Артина

Пусть Ω — поле. Для всякой части V поля Ω множество $\mathscr{F}(V, \Omega) = \Omega^V$ отображений V в Ω снабжено структурой *векторного пространства над* Ω, относительно которой произведение αu элемента $\alpha \in \Omega$ и отображения u части V в Ω является отображением $x \to \alpha u(x)$ (гл. II, § 1, n° 4). *Рангом* над Ω части множества $\mathscr{F}(V, \Omega)$ является, таким образом, размерность векторного подпространства в $\mathscr{F}(V, \Omega)$, порожденного этой частью (гл. II, § 3, n° 2).

Поле Ω обладает структурой *векторного пространства над* K. Мы будем обозначать символом Ω_K множество Ω, снабженное только этой структурой векторного пространства. Когда мы будем говорить об *автоморфизмах* Ω, то речь будет идти всегда об автоморфизмах структуры *поля* Ω.

Предложение 1. *Пусть K — некоторое подполе поля Ω, V — векторное подпространство пространства Ω_K размерности n (над K). Тогда совокупность $\mathscr{L}(V, \Omega_K)$ всевозможных K-линейных*

отображений пространства V в Ω_K является векторным пространством размерности n (над Ω).

Прежде всего, ясно, что если u — K-линейное отображение пространства V в Ω_K, то αu для любого $\alpha \in \Omega$ также будет K-линейным отображением пространства V в Ω_K и, следовательно, $\mathscr{L}(V, \Omega_K)$ является векторным подпространством пространства $\mathscr{F}(V, \Omega)$. Пусть $(a_i)_{1 \leqslant i \leqslant n}$ — базис пространства V над полем K, и пусть u_i $(1 \leqslant i \leqslant n)$ — линейные отображения V в Ω_K, определяемые условиями $u_i(a_j) = \delta_{ij}$ (символ Кронекера). Эти отображения линейно независимы, так как соотношение $\sum_{k=1}^{n} \alpha_k u_k(x) = 0$ для всех $x \in V$, примененное к $x = a_j$, влечет $\alpha_j = 0$. С другой стороны, пусть u — произвольное линейное отображение пространства V в Ω_K; полагая $u(a_i) = \beta_i$ $(1 \leqslant i \leqslant n)$, получаем, что отображение $u - \sum_{k=1} \beta_k u_k$ равно нулю для всех a_j, следовательно, равно нулю на V, т. е. $u = \sum_{k=1}^{n} \beta_k u_k$. Таким образом, отображения u_i $(1 \leqslant i \leqslant n)$ образуют *базис* пространства $\mathscr{L}(V, \Omega_K)$ над полем Ω.

Следствие. *Ранг (над Ω) множества ограничений на V всех K-автоморфизмов поля Ω не превосходит размерности пространства V над полем K.*

Действительно, ограничение на V любого K-автоморфизма поля Ω является K-линейным отображением пространства V в Ω_K.

Напомним, что для всякого множества автоморфизмов $\mathscr{A}$ поля Ω множество элементов этого поля, *инвариантных* при всех автоморфизмах $u \in \mathscr{A}$, является *подполем* Ω и называется *полем инвариантов относительно* $\mathscr{A}$ (гл. II, § 5, n° 6).

Теорема 1 (Артин). *Пусть Ω — поле, $\mathscr{G}$ — множество его автоморфизмов, обладающее следующими свойствами: 1° если $u \in \mathscr{G}$ и $v \in \mathscr{G}$, то $u \circ v \in \mathscr{G}$; 2° тождественный автоморфизм принадлежит $\mathscr{G}$. Пусть K — поле, инвариантов относительно $\mathscr{G}$. Для того чтобы часть V поля Ω имела конечный ранг n над полем K, необходимо и достаточно, чтобы множество $\mathscr{G}_V$ ограничений на V элементов множества $\mathscr{G}$ имело ранг n над полем Ω.*

Можно ограничиться случаем, когда V — *векторное подпространство* пространства Ω_K. В самом деле, пусть V_0 — векторное

подпространство Ω_K, порожденное множеством V; тогда, для того чтобы некоторое K-линейное отображение u части V в поле Ω было нулевым, необходимо и достаточно, чтобы $u(x)=0$ для всех $x\in V$. Следовательно, ранг множества $\mathscr{G}_V$ над полем K равен рангу множества $\mathscr{G}_{V_0}$ над K.

Пусть теперь V — векторное подпространство пространства Ω_K конечной размерности m над K. Ввиду следствия из предложения 1 множество $\mathscr{G}_V$ имеет ранг, не превосходящий m. Остается доказать, что если V — векторное подпространство пространства Ω_K, для которого множество $\mathscr{G}_V$ имеет конечный ранг n над Ω, то V имеет размерность над K, *не меньшую* n. Пусть (b_i) $(1\leqslant i\leqslant n+1)$ — семейство из $n+1$ произвольных элементов пространства V. Мы покажем, что это семейство *связано* в Ω_K, что и будет доказательством нашего утверждения. Пусть $\mathscr{A}$ — векторное пространство на Ω_K, порожденное множеством $\mathscr{G}_V$. Рассмотрим линейное отображение $u\longrightarrow(u(b_i))$ пространства $\mathscr{A}$ в векторное пространство Ω^{n+1}. Ранг этого отображения не превосходит n, так как размерность $\mathscr{A}$ равна n; образ W пространства $\mathscr{A}$ при этом отображении, следовательно, является подпространством пространства Ω^{n+1}, *отличным* от Ω^{n+1}. Для любого автоморфизма $v\in\mathscr{G}$ обозначим символом $\bar{v}$ отображение пространства Ω^{n+1} в себя, определяемое соотношением $\bar{v}((x_i))=(v(x_i))$. Для всякого элемента $u\in A$ имеем тогда $\bar{v}((u(b_i)))=(v(u(b_i)))$. Но $v\circ u\in\mathscr{A}$, ибо u есть ограничение на V отображения $\sum_\lambda a_\lambda u_\lambda$, где $u_\lambda\in\mathscr{G}$, следовательно, $v\circ u$ совпадает с ограничением на V отображения $\sum_\lambda v(a_\lambda)(v\circ u_\lambda)$ и, по предположению, $v\circ u_\lambda\in\mathscr{G}$. Таким образом, по определению W, мы имеем $\bar{v}(W)\subset W$ для всех $v\in\mathscr{G}$. Отсюда следует, что подполе Ω, *связанное с* W (для канонического базиса пространства Ω^{n+1}) содержится в поле K *инвариантов* относительно $\mathscr{G}$ (гл. II, § 5, предложение 10). Итак, существует система уравнений, определяющих W с коэффициентами в поле K (гл. II, § 5, теорема 2), и так как $W\neq\Omega^{n+1}$, то существует семейство $(\beta_i)_{1\leqslant i\leqslant n+1}$ элементов из K, из которых не все равны нулю и таких, что $\sum_{i=1}^{n+1}\beta_i u(b_i)=0$ для *всех* $u\in\mathscr{A}$. Взяв в качестве u ограничение на V тождест-

венного автоморфизма (который, по предположению, принадлежит $\mathcal{G}$), мы получим $\sum_{i=1}^{n+1} \beta_i b_i = 0$, что и завершает доказательство.

Эту теорему легко распространить на произвольные *некоммутативные тела* (упражнение 2); тогда она оказывается обобщением теоремы 3б) гл. II, § 5, откуда мы скопировали доказательство.

2. *Сепарабельные расширения*

Пусть E — некоторое расширение поля K, Ω — *алгебраически замкнутое* расширение поля E. Следствие из предложения 1 показывает, что для любого подпространства V пространства Ω_K, содержащегося в E и имеющего конечную размерность, множество ограничений на V всех K-автоморфизмов поля Ω имеет ранг (над Ω), *не превосходящий* размерности пространства V (над K).

Определение 1. *Расширение E поля K называется сепарабельным (над K), если существует алгебраически замкнутое расширение Ω поля E, обладающее следующим свойством:*

(S) Для всякого векторного подпространства V пространства Ω_K, содержащегося в E и имеющего конечную размерность, множество ограничений на V всех K-автоморфизмов поля Ω имеет ранг (над Ω), равный размерности V (над K).

Ввиду предложения 1 это равносильно утверждению, что для всякого векторного подпространства $V \subset E$ конечной размерности над K любое K-линейное отображение пространства V в Ω_K является линейной комбинацией (с коэффициентами в Ω) ограничений на V K-автоморфизмов поля Ω.

Замечание. Условие сепарабельности E над K выражается еще следующим образом: для произвольной свободной над K системы, состоящей из конечного числа n элементов a_i расширения E $(1 \leqslant i \leqslant n)$, существует n K-автоморфизмов u_i расширения Ω $(1 \leqslant i \leqslant n)$ таких, что определитель $\det(u_i(a_j))$ не равен нулю. Действительно, пусть V — векторное подпространство поля E, порожденное элементами a_i. Размерность пространства V над полем K равна n, и предыдущее свойство означает, что система уравнений $\sum_{i=1}^{n} \xi_i u_i(a_j) = 0$ $(1 \leqslant j \leqslant n)$ имеет только тривиальное решение в Ω, т. е. что ограничения u_i на V линейно независимы над Ω.

ТЕОРЕМА 2. *Для того чтобы расширение E поля K было сепарабельным над K, необходимо и достаточно, чтобы в алгебраическом замыкании Ω_0 поля E поле E было линейно разделено (над K) с полем инвариантов относительно группы K-автоморфизмов поля Ω_0. Если это условие выполнено, то всякое алгебраически замкнутое расширение Ω поля E обладает свойством (S).*

Действительно, пусть Ω — алгебраически замкнутое расширение поля E, $L(\Omega)$ — поле элементов, инвариантных относительно группы K-автоморфизмов поля Ω. В силу теоремы 1 свойство (S) означает, что для любой конечной части расширения E ранг этой части над K равен рангу ее над $L(\Omega)$, иначе говоря, всякая часть расширения E, свободная над K, является свободной над $L(\Omega)$. Это в свою очередь означает, что поля E и $L(\Omega)$ *линейно разделены* над K (§ 2, n° 3). Пусть Ω_0 — алгебраическое замыкание расширения E в поле Ω; теорема будет доказана, если мы докажем, что $L(\Omega) = L(\Omega_0)$. Но это вытекает из следующего более точного результата:

ПРЕДЛОЖЕНИЕ 2. *Пусть Ω — алгебраически замкнутое расширение поля K, и пусть $\overline{K}$ — алгебраическое замыкание поля K в Ω; тогда $L(\Omega) = L(\overline{K})$.*

Действительно, всякий элемент $x \in L(\Omega)$ алгебраичен над полем K (§ 5, следствие из предложения 3), следовательно, принадлежит $\overline{K}$. С другой стороны, всякий K-автоморфизм поля $\overline{K}$ продолжается до некоторого K-автоморфизма поля Ω (§ 6, следствие 1 из предложения 2), следовательно, x должен быть инвариантным при всех K-автоморфизмах поля $\overline{K}$, так что $L(\Omega) \subset L(\overline{K})$. Обратно, поскольку $\overline{K}$ — алгебраическое замыкание поля K (§ 4, следствие из предложения 1), оно является нормальным расширением K, следовательно, ограничение на $\overline{K}$ всякого K-автоморфизма поля Ω есть автоморфизм $\overline{K}$ (§ 6, предложение 6). Поэтому всякий элемент поля $L(\overline{K})$ инвариантен при всех K-автоморфизмах поля Ω, чем завершается доказательство тождества $L(\overline{K}) = L(\Omega)$.

Мы уточним этот результат в § 8, n° 1, полностью описав поле $L(\overline{K})$. Сейчас мы можем сказать, что поле $L(\overline{K})$ состоит

из тех алгебраических над K элементов, которые *совпадают со всеми своими сопряженными* (т. е. из алгебраических элементов, минимальный многочлен которых над полем K имеет *только один* корень).

3. *Примеры сепарабельных расширений. Совершенные поля*

Предложение 3. *Всякое чисто трансцендентное расширение поля K является сепарабельным над K.*

Действительно, известно (§ 5, следствие из предложения 11), что такое расширение E линейно разделено со всяким алгебраическим расширением поля K, и в частности, с полем инвариантных элементов $L(\overline{K})$ относительно группы K-автоморфизмов алгебраического замыкания $\overline{K}$ поля K в алгебраическом замыкании Ω_0 поля E. Следовательно, предложение вытекает из теоремы 2 и предложения 2.

Определение 2. *Поле K называется совершенным, если оно совпадает с множеством элементов, инвариантных относительно группы K-автоморфизмов алгебраического замыкания поля K.*

Предложение 4. *Если поле K совершенно, то всякое его расширение сепарабельно (над K); обратно, если всякое алгебраическое расширение поля K сепарабельно, то K — совершенное поле.*

Предложение является следствием теоремы 2 и предложения 2.

Предложение 5. *Для того чтобы поле K, имеющее характеристическую экспоненту p, было совершенным, необходимо и достаточно, чтобы выполнялось условие $K^p = K$.*

Условие *необходимо*: действительно, пусть Ω — алгебраическое замыкание поля K, x — произвольный элемент поля K, y — такой элемент поля Ω, что $y^p = x$. Для любого K-автоморфизма u расширения Ω имеем $(u(y))^p = x$ и, следовательно, $(u(y))^p = y^p$, откуда $u(y) = y$ (§ 1, предложение 1). Поскольку поле K совершенно, $y \in K$, т. е. $K^p = K$.

Условие *достаточно*: действительно, если оно выполнено, то подкольцо $K[X^p]$ кольца $K[X]$ равно $K^p[X^p]$, следовательно, совпадает с $(K[X])^p$ (§ 1, предложение 2). Пусть элемент $x \in \Omega$ инвариантен относительно всех K-автоморфизмов поля Ω, тогда x алгебраичен над K, и его минимальный многочлен f над K

не имеет других корней, кроме x. Если $x \notin K$, то многочлен f должен иметь степень больше 1, следовательно, иметь кратный корень. Это невозможно при $p=1$, а при $p>1$ из этого вытекает включение $f \in K[X^p]$ (§ 3, предложение 1), но, как было только что замечено, тогда $f=g^p$, где $g \in K[X]$, что невозможно, так как f неприводим.

Следствие. *Если поле K конечно или алгебраически замкнуто или имеет характеристику нуль, то оно совершенно. В частности, всякое простое поле совершенно.*

Следствие очевидно в случае, когда поле K имеет характеристику 0, так как отображение $x \longrightarrow x^p$ (p — характеристическая экспонента поля K) является тождественным. Если K — конечное поле, то $x \longrightarrow x^p$ — взаимно однозначное отображение K в себя (§ 1, предложение 1), следовательно, отображает K *на* себя. Наконец, если поле K алгебраически замкнуто, то для любого элемента $x \in K$ уравнение $y^p=x$ имеет корень в K.

Если K_0 — поле характеристики $p>0$, то поле $K=K_0(X)$ рациональных дробей от одной переменной над K_0 *не является совершенным полем*: в самом деле, не существует элемента $u(X)/v(X)$, принадлежащего полю K (u и v — многочлены кольца $K_0[X]$) и такого, что $(u(x)/v(x))^p=X$. Действительно, последнее соотношение можно записать в виде $X(v(X))^p=(u(X))^p$; обозначая через m и n степени многочленов u и v, соответственно получим $mp=np+1$, что невозможно. Кроме того, если Ω — алгебраическое замыкание поля K, z — корень многочлена Y^p-X (кольца $K[Y]$) в поле Ω, то расширение $K(z)$ не сепарабельно над K, так как всякий сопряженный с z над K элемент совпадает с z. Этим доказано, что единственным K-изоморфизмом поля $K(z)$ в поле Ω является тождественный автоморфизм.

4. *Свойства сепарабельных расширений*

Предложение 6. *Если расширение E поля K сепарабельно над K, то всякое подрасширение расширения E сепарабельно над K. Обратно, если E — такое расширение поля K, что всякое его подрасширение конечного типа сепарабельно над K, то E сепарабельно над K.*

Предложение тотчас следует из определения 1, так как всякое подрасширение расширения E, порожденное векторным подпространством конечной размерности, имеет конечный тип.

Таким образом, можно говорить, что сепарабельность является свойством «конечного характера».

Предложение 7. *Пусть F — расширение поля K, E — подрасширение поля F. Если E сепарабельно над K и F сепарабельно над E,* то *F сепарабельно над $\bar{K}$.*

Действительно, пусть Ω — алгебраическое замыкание поля F, L — поле элементов, инвариантных относительно всех K-автоморфизмов расширения Ω, M — поле элементов, инвариантных относительно E-автоморфизмов поля Ω. Так как всякий элемент поля L инвариантен относительно всех E-автоморфизмов поля Ω, имеет место включение $E(L) \subset M$ (рис. 2). По предположению,

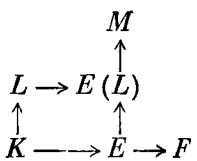

Рис. 2.

поля F и M линейно разделены над E, следовательно, F и $E(L)$ линейно разделены над E, и так как, кроме того, E и L линейно разделены над K, то F и L линейно разделены над K (§ 2, предложение 7), откуда, применяя теорему 2, получим предложение.

Если поле F сепарабельно над K, то F не обязательно сепарабельно над любым *подрасширением* поля F (см. § 8, предложение 5). Например, если K — поле характеристики $p > 0$, то поле $F = K(X)$ рациональных дробей от одной переменной над K сепарабельно над K (предложение 3), но не сепарабельно над подрасширением $E = K(X^p)$ (см. п° 3).

5. *Теорема Дедекинда*

Теорема 3 (Дедекинд). *Пусть Ω — расширение поля K, E — подрасширение Ω. Любое семейство $(u_\lambda)_{\lambda \in L}$ попарно различных K-изоморфизмов поля E в Ω состоит из линейно независимых (над Ω) отображений.*

Будем рассуждать от противного. Если отображения u_λ линейно зависимы над Ω, то между ними существует *первичное*

соотношение $\sum_\lambda \alpha_\lambda u_\lambda = 0$ (гл. II, § 5, n°4); иначе говоря, $\sum_\lambda \alpha_\lambda u_\lambda(x) = 0$ для всех $x \in E$. Для любых элементов $x \in E$ и $y \in E$, также $yx \in E$, так как E — поле, откуда

$$\sum_\lambda \alpha_\lambda u_\lambda(yx) = 0,$$

и так как u_λ — изоморфизмы поля E, то

$$\sum_\lambda \alpha_\lambda u_\lambda(y)\, u_\lambda(x) = 0$$

при любых x и y, принадлежащих E. Это означает, что для всякого элемента $y \in E$ элементы $\alpha_\lambda u_\lambda(y)$ являются коэффициентами линейных соотношений между отображениями u_λ. Так как $\sum \alpha_\lambda u_\lambda = 0$ — первичное соотношение, для любого элемента $y \in E$ существует такой элемент $\varrho(y) \in E$, что для *всех* $\lambda \in L$ справедливы тождества

$$\alpha_\lambda u_\lambda(y) = \varrho(y)\, \alpha_\lambda$$

(гл. II, § 5, предложение 2). Следовательно, если μ и ν — различные индексы из L такие, что $\alpha_\mu \neq 0$ и $\alpha_\nu \neq 0$, то $u_\mu(y) = u_\nu(y)$ для всех $y \in E$ в противоречии с предположением. Следовательно, существует только один индекс $\mu \in L$ такой, что $\alpha_\mu \neq 0$, но из рассмотренного соотношения между u_λ вытекает тогда, что $u_\mu = 0$, что невозможно.

Замечание. Те же рассуждения применимы к более общему случаю, когда u_λ — *представления мультипликативного моноида* E в поле Ω (снабженное только мультипликативным законом); если отображения u_λ попарно различны и отличны от нуля, то они линейно независимы в векторном пространстве Ω^E отображений E в Ω.

Предложение 8. *Пусть* Ω — *алгебраически замкнутое расширение поля* K, E — *подрасширение* Ω *конечной степени над* K. *Число* K-*изоморфизмов поля* E *в* Ω *не превосходит степени* E *над* K. *Для того чтобы оно было равно степени поля* E *над* K, *необходимо и достаточно, чтобы расширение* E *было сепарабельным над* K.

Первая часть предложения тотчас следует из теоремы 3, так как размерность над Ω векторного пространства $\mathscr{L}(E, \Omega_K)$ равна $[E : K]$ (предложение 1). Если E сепарабельно над K, то

множество ограничений на E K-автоморфизмов поля Ω имеет ранг $[E:K]$ над Ω, следовательно, состоит не менее чем из $[E:K]$ элементов. Обратно, если существует $[E:K]$ различных K-изоморфизмов поля E в Ω, то они являются ограничениями на E K-автоморфизмов поля Ω (§ 6, следствие 2 из предложения 2) и линейно независимы над Ω (теорема 3). Ввиду теоремы 1 поле E имеет ранг $[E:K]$ над полем $L(\Omega)$ элементов, инвариантных относительно группы K-автоморфизмов поля Ω. Этим доказано, что поля E и $L(\Omega)$ линейно разделены над K (§ 2, n° 3), и следовательно (теорема 2), что расширение E сепарабельно над K.

6. *Сепарабельные алгебраические элементы*

Определение 3. *Пусть E — расширение поля K. Элемент x расширения E, алгебраический над K, называется сепарабельным над K, если алгебраическое расширение $K(x)$ сепарабельно над K.*

Предложение 9. *Пусть Ω — алгебраически замкнутое расширение поля K. Для того чтобы алгебраический элемент $x \in \Omega$ степени n над K был сепарабельным над K, необходимо и достаточно, чтобы он имел n различных сопряженных элементов над K (или, что то же, ввиду предложения 3 § 6, чтобы все корни в Ω минимального многочлена элемента x над K были простыми).*

Действительно (§ 6, n° 2), число K-изоморфизмов расширения $K(x)$ равно числу элементов, сопряженных с x, а степень поля $K(x)$ над K равна n.

Следствие 1. *Если элемент $x \in \Omega$, алгебраический над K, является сепарабельным над K, то всякий сопряженный с ним над K элемент тоже сепарабелен над K.*

Следствие 2. *Если элемент $x \in \Omega$ является простым корнем некоторого многочлена $g \in K[X]$, то x сепарабелен над K.*

Действительно, минимальный многочлен f элемента x над полем K делит g (§ 3, теорема 1), следовательно, x — простой корень многочлена f, и то же верно для всех сопряженных с x (§ 6, предложение 3).

Следствие 3. *Если элемент $x \in \Omega$ алгебраичен и сепарабелен над полем K, то он сепарабелен над любым расширением F поля K, содержащемся в Ω.*

Действительно, x — простой корень своего минимального многочлена над K, принадлежащего кольцу $F[X]$.

Назовем многочлен кольца $K[X]$ *сепарабельным*, если все его корни в алгебраическом замыкании поля K сепарабельны. Ввиду предложения 1 § 3, *для того чтобы неприводимый многочлен $f \in K[X]$ был сепарабельным, необходимо и достаточно*, чтобы $f \notin K[X^p]$ (p — характеристика поля K). В частности, *если K — поле характеристики нуль, то всякий непостоянный многочлен кольца $K[X]$ сепарабелен.*

Предложение 10. *Пусть Ω — алгебраически замкнутое расширение поля K. Пусть A — часть Ω, состоящая из сепарабельных алгебраических элементов над K. Тогда $K(A)$ — сепарабельное алгебраическое расширение поля K.*

Достаточно доказать, что для всякой конечной части F поля $K(A)$ поле $K(F)$ сепарабельно (предложение 6). Так как каждый элемент части F содержится в некотором расширении поля K, получаемом присоединением конечной части множества A, то все поле $K(F)$ содержится в поле $K(B)$, где B — некоторая конечная часть множества A и, следовательно, можно ограничиться случаем, когда множество A конечно. Итак, пусть $(a_i)_{1 \leqslant i \leqslant n}$ — некоторая конечная последовательность сепарабельных алгебраических элементов расширения Ω поля K. Будем доказывать индукцией по n, что поле $K(a_1, a_2, \ldots, a_n)$ сепарабельно над K. Ввиду определения 3 предложение верно для $n = 1$. Так как элемент a_n сепарабелен над полем $K(a_1, a_2, \ldots, a_{n-1})$ (следствие 3 из предложения 9), расширение $K(a_1, a_2, \ldots, a_n)$ сепарабельно над $K(a_1, \ldots, a_{n-1})$ (определение 3); но, по предположению индукции, поле $K(a_1, \ldots, a_{n-1})$ сепарабельно над K, следовательно, и поле $K(a_1, a_2, \ldots, a_n)$ сепарабельно над K (предложение 7).

Следствие 1. *Для того чтобы алгебраическое расширение E поля K было сепарабельным, необходимо и достаточно, чтобы все элементы поля E были сепарабельны над K.*

Следствие 2. *Всякое алгебраическое расширение совершенного поля K совершенно.*

Действительно, пусть E — алгебраическое расширение поля K, F — алгебраическое расширение поля E; всякий элемент x расширения F алгебраичен над K (§ 3, предложение 8), следовательно, сепарабелен над K по предположению о совершенности

(предложение 4). Отсюда вытекает, что x сепарабелен над E (следствие 3 из предложения 9) и, следовательно, F — сепарабельное расширение поля E (следствие из предложения 10), но это значит, что E совершенно (предложение 4).

Предложение 11. *В любом алгебраическом расширении E поля K множество E_0 элементов этого поля, сепарабельных над K, является сепарабельным расширением поля K, которое совпадает с объединением всех сепарабельных расширений поля K, содержащихся в E.* Действительно, поле $K(E)$ сепарабельно над K (предложение 10), следовательно, $K^0(E_0) \subset E_0$ и, значит, $K(E_0) = E_0$.

7. *Примитивные элементы*

Пусть дано алгебраическое расширение E поля K конечной степени n. Элемент $x \in E$ называется *примитивным элементом* расширения E, если $E = K(x)$: существование примитивного элемента означает тем самым, что E — *простое* расширение поля K. Элемент x, следовательно, имеет степень n над K; обратно, всякий элемент расширения E, степень которого равна n, является примитивным элементом расширения E (§ 2, следствие 2 из теоремы 1).

Предложение 12. *Пусть K — бесконечное поле, тогда всякое сепарабельное алгебраическое расширение E поля K конечной степени является простым.*

Пусть $[E:K] = n$; по предположению, существует n различных K-изоморфизмов u_i $(1 \leqslant i \leqslant n)$ расширения E в поле Ω (предложение 8). Пусть V_{ij} $(i \neq j)$ — множество тех элементов $y \in E$, для которых $u_i(y) = u_j(y)$; тогда V_{ij} — подполе поля E, содержащее K и, следовательно, являющееся векторным подпространством пространства E (над K). По предположению, множество V_{ij} отлично от E, и так как поле K бесконечно, то существует элемент $x \in E$, не принадлежащий ни к одному из $n(n-1)/2$ векторных подпространств V_{ij} (гл. IV, § 2, предложение 8); это значит, что все элементы $u_i(x)$ различны $(1 \leqslant i \leqslant n)$, следовательно, x имеет по крайней мере n различных сопряженных в Ω, т. е. степень x над K не меньше n, и так как $x \in E$, то степень x равна n, т. е. $E = K(x)$.

Мы увидим в § 11, что предложение 12 распространяется на случай *конечного* поля K (§ 11, предложение 4).

Упражнения. 1) Пусть f — неприводимый многочлен кольца $K[X]$, сепарабельный над K, и пусть α_i $(1 \leqslant i \leqslant n)$ — его корни в алгебраическом замыкании Ω поля K. Пусть g — произвольный многочлен кольца $K[X]$, h — некоторый неприводимый множитель (в $K[X]$) многочлена $f(g(X))$. Доказать, что степень многочлена h является целым кратным rn числа n и что h имеет точно r общих корней с каждым из многочленов $g(X) - \alpha_i$ кольца $\Omega[X]$ (рассмотреть сопряженные произвольного корня многочлена h).

*2) Пусть Ω — тело (*не обязательно коммутативное*), K — подтело тела Ω, Ω_K — множество Ω, снабженное структурой *правого* векторного пространства над K. Для любого векторного подпространства V пространства Ω_K рассмотрим множество $\mathscr{L}(V, \Omega_K)$ линейных отображений пространства V в Ω, снабженное структурой *левого* векторного пространства над Ω, индуцированной структурой Ω_S^V (см. гл. II, § 5, n° 6).

а) Доказать, что если V имеет размерность n над K, то размерность пространства $\mathscr{L}(V, \Omega_K)$ над Ω равна n.

б) Пусть G — некоторое множество автоморфизмов тела Ω, содержащее тождественный автоморфизм и такое, что если $u \in G$, $v \in G$, то $u \circ v \in G$. Пусть L — тело элементов, инвариантных относительно G. Для того чтобы векторное подпространство V пространства Ω_L имело конечную размерность n над L, необходимо и достаточно, чтобы множество G_V ограничений на V элементов G имело ранг n над Ω (то же доказательство, что для теоремы 1).

в) Пусть K — некоторое подтело тела Ω; назовем векторное подпространство V пространства Ω_K конечной размерности n сепарабельным над K, если любое линейное отображение пространства V в Ω_K является линейной комбинацией (с коэффициентами из Ω) ограничений на V K-автоморфизмов тела Ω. Для того чтобы V было сепарабельным, необходимо и достаточно, чтобы его ранг (справа) над полем инвариантных элементов относительно K-автоморфизмов тела Ω был равен n; вывести отсюда, что всякое векторное подпространство пространства V сепарабельно.

г) Пусть E — подтело тела Ω, содержащее K. Будем говорить, что E сепарабельно над K, если всякое векторное подпространство пространства E конечной (правой) размерности над K сепарабельно над K. Доказать, что если в цепочке $K \subset E \subset F \subset \Omega$ тело E сепарабельно над K, а F сепарабельно над E, то F сепарабельно над K.

д) Пусть E — подтело тела Ω, содержащее K, и пусть $(u_\iota)_{\iota \in I}$ — некоторое семейство K-изоморфизмов тела E в Ω. Для того чтобы отображения u_ι были линейно зависимы (над Ω), необходимо и достаточно, чтобы существовали K-изоморфизм v пространства E в Ω,

конечная непустая часть J множества I и семейство $(\mu_i)_{i\in J}$ не равных нулю элементов тела Ω такие, что $\sum_{i\in J}\mu_i=0$ и $u_i(x)=\mu_i v(x)\mu_i^{-1}$ для всех $i\in J$ и всех $x\in E$.

§ 8. Радикальные элементы. Критерий сепарабельности

В этом параграфе Ω — алгебраически замкнутое поле характеристической экспоненты p; все предложения, доказываемые в этом параграфе, тривиальны для $p=1$.

1. Радикальные элементы

Предложение 1. *Пусть K — некоторое подполе поля Ω. Для того чтобы элемент $x\in\Omega$ был инвариантен при всех K-автоморфизмах поля Ω, необходимо и достаточно, чтобы существовало целое число $m\geqslant 0$ такое, что $x^{p^m}\in K$. Пусть e — наименьшее из этих чисел; тогда минимальный многочлен элемента x над K имеет вид $X^{p^e}-x^{p^e}$.*

Условие достаточно; в самом деле, пусть u — произвольный K-автоморфизм поля Ω. Если $x^{p^m}\in K$, то $(u(x))^{p^m}=u(x^{p^m})=x^{p^m}$, следовательно (§ 1, следствие из предложения 1), $u(x)=x$. Обратно, если элемент x инвариантен относительно всех K-автоморфизмов поля Ω, то x алгебраичен над K, и его минимальный многочлен f над K имеет только один корень (§ 6, предложение 3). При $p=1$, как мы уже видели $x\in K$ (§ 3, предложение 1); если же $p>1$, то пусть e — наибольшее из чисел h, для которых $f\in K[X^{p^h}]$. Имеем $f(X)=g[X^{p^e}]$, где многочлен $g\in K[X]$, очевидно, неприводим и $g\notin K[X^p]$. Так как g имеет только один корень x^{p^e} в Ω, то $g(X)=X-x^{p^e}$ (§ 3, предложение 1). Предложение доказано.

Определение 1. *Пусть дано подполе K поля Ω; элемент $x\in\Omega$ называется радикальным над K, если существует такое целое число $m\geqslant 0$, что $x^{p^m}\in K$.*

Множество радикальных над K элементов поля Ω является, таким образом, *полем элементов, инвариантных* относительно всех K-автоморфизмов поля Ω (см. § 7, п° 2); ввиду предложения 1 это поле можно определить как множество корней всех многочленов вида $X^{p^e}-a$ кольца $K[X]$ (e — произвольное неотрицательное число).

Так как поле Ω алгебраически замкнуто, то оно совершенно (§ 7, следствие из предложения 5), следовательно, отображение $x \longrightarrow x^{p^e}$ является автоморфизмом Ω. Мы будем обозначать символом $x \longrightarrow x^{p^{-e}}$ или $x \longrightarrow x^{1/p^e}$ обратный автоморфизм, а символом $K^{p^{-e}}$ или K^{1/p^e} — образ поля K при отображении $x \longrightarrow x^{p^{-e}}$ поля K в Ω. Поле $K^{p^{-e}}$ является множеством корней многочленов $X^{p^e} - a$ кольца $K[X]$, следовательно, оно является *алгебраическим* расширением поля K, имеющим, возможно, *бесконечную* степень. Если $e \leqslant f$, то $K^{p^{-e}} \subset K^{p^{-f}}$. Подполе поля Ω, состоящее из радикальных над K элементов, является объединением полей $K^{p^{-e}}$ при e, пробегающем все неотрицательные числа. Будем обозначать это поле символом $K^{p^{-\infty}}$; оно является алгебраическим расширением поля K (см. § 7, предложение 2).

Предложение 2. *Поле $K^{p^{-\infty}}$ является наименьшим совершенным подполем поля Ω, содержащим K.*

Действительно, пусть E — произвольное совершенное подполе поля Ω, содержащее K; тогда $E^{p^{-e}} = E$ для всех $e \geqslant 0$ (§ 7, предложение 5), следовательно, $E \supset K^{p^{-e}}$ и, значит, $E \supset K^{p^{-\infty}}$. Обратное непосредственно следует из того, что всякий K-автоморфизм поля Ω является $K^{p^{-\infty}}$-автоморфизмом, следовательно, $K^{p^{-\infty}}$ является полем элементов, инвариантных относительно всех $K^{p^{-\infty}}$-автоморфизмов поля Ω, т. е. поле $K^{p^{-\infty}}$ совершенно.

Замечание. Если поле K не совершенно, то все поля $K^{p^{-e}}$ различны, так как тогда $K^p \neq K$ (§ 7, предложение 5) и изоморфизм $x \longrightarrow x^{p^{-e}}$ поля K на $K^{p^{-e}}$ отображает K^p на $K^{p^{-(e-1)}}$. Поле $K^{p^{-\infty}}$ является, таким образом, алгебраическим расширением *бесконечной* степени над K, когда K не совершенно.

2. Критерий Маклейна

Предложение 3 (Маклейн). *Пусть K — некоторое подполе поля Ω, $E \subset \Omega$ — расширение поля K. Для того чтобы E было сепарабельным над K, необходимо, чтобы поля E и $K^{p^{-\infty}}$ были линейно разделены над K, и достаточно, чтобы поля E и $K^{p^{-1}}$ были линейно разделены над K.*

Критерий сепарабельности (§ 7, теорема 2) означает, что E и $K^{p^{-\infty}}$ линейно разделены над K. Следовательно, остается доказать, что если поля E и $K^{p^{-1}}$ линейно разделены над K, то линейно разделены поля E и $K^{p^{-\infty}}$. Действительно, всякое семейство (a_ι) элементов поля E, свободное над K, свободно над $K^{p^{-1}}$, следовательно, семейство (a_ι^p) свободно над K и по индукции семейство $(a_\iota^{p^f})$ свободно над K для всех неотрицательных чисел f. Таким образом, соотношение вида $\sum_\iota \mu_\iota a_\iota = 0$, где $\mu_\iota \in K^{p^{-\infty}}$ все равны нулю, кроме конечного числа, эквивалентно соотношению $\sum_\iota \mu_\iota^{p^f} a_\iota^{p^f} = 0$ для всех положительных чисел f. Так как существует число f такое, что $\mu_\iota^{p^f} \in K$ для всех ι, то $\mu_\iota = 0$ для всех ι, и предложение доказано.

Следствие. *Пусть E — некоторое расширение поля K. Если E сепарабельно над K, то для любого линейно свободного над K семейства (a_ι) элементов расширения E, семейство (a_ι^p) линейно свободно над K. Обратно, если существует линейный базис (b_λ) расширения E над K такой, что семейство b_λ^p линейно свободно над K, то E сепарабельно над K.*

Это утверждение непосредственно следует из критерия линейной разделенности (§ 2, n° 3).

Замечание. Если поле E сепарабельно над K, то из предложения 3 вытекает, что $E \cap K^{p^{-\infty}}$. Однако может существовать алгебраическое расширение E поля K, не сепарабельное над K и такое, что $E \cap K^{p^{-\infty}} = K$ (см. упражнение 17 и § 10, предложение 14).

3. *Приложение к сепарабельным алгебраическим расширениям*

Предложение 4. *Пусть A — некоторое множество алгебраических элементов над полем K, и пусть поле $K(A)$ сепарабельно над K. Тогда $K(A^p) = K(A)$. Обратно, если A имеет конечный ранг над K и $K(A^p) = K(A)$, то $K(A)$ сепарабельно над K.*

Будем предполагать сначала, что A имеет *конечный* ранг над полем K и $(a_i)_{1\leqslant i\leqslant u}$ — линейный базис пространства $K(A)$ над K. Тогда $K(A)=K[A]$ и $K(A^p)=K[A^p]$ (§ 3, предложение 3), следовательно, элементы a_i^p являются системой образующих векторного пространства $K(A^p)$ над полем K (§ 1, предложение 3). Если расширение $K(A)$ сепарабельно над K, то элементы a_i^p линейно независимы над K (следствие из предложения 3), следовательно, $[K(A^p):K]=[K(A):K]$ и $K(A^p)=K(A)$. Обратно, если выполнено это условие, то элементы a_i^p линейно независимы над K (гл. II, § 3, следствие 2 из теоремы 3), следовательно, расширение $K(A)$ сепарабельно над K (следствие из предложения 3). Если же множество A имеет бесконечный ранг над полем K, то расширение $K(A)$ является объединением подполей $K(F)$, где F пробегает множество конечных частей множества A (§ 2, следствие из предложения 3). Если поле $K(A)$ сепарабельно над K, то любое подполе $K(F)$ сепарабельно над K, следовательно, $K(F^p)=K(F)$ и поле $K(A^p)$, являясь объединением полей $K(F^p)$, совпадает с $K(A)$.

Следствие. *Пусть E — некоторое сепарабельное алгебраическое расширение поля K; если система (b_λ) образует базис поля E над K, то система (b_λ^p) тоже образует базис E над K.*

Действительно, семейство (b_λ^p) линейно свободно над K (следствие из предложения 3), следовательно, оно является базисом пространства $K[E^p]$ над K (§ 1, предложение 3). Так как расширение E алгебраично над K, имеем $K(E^p)=K[E^p]=E$ (§ 3, предложение 3).

Замечания. 1) Используя предложение 4, можно дать другое доказательство того, что всякий сепарабельный алгебраический над K элемент x будет сепарабельным над любым расширением F поля K, содержащимся в Ω (§ 7, следствие 3 из предложения 9): действительно,

$$F(x^p)=K(F)(x^p)=K(x^p)(F)=K(F)(x)=F(x).$$

2) Если E — алгебраическое расширение *бесконечной* степени поля K, то условие $K(E^p)=E$ не является достаточным для того, чтобы E было сепарабельным над K: например, поле $E=K^{p^{-\infty}}$ удовлетворяет этому условию.

Предложение 5. *Пусть E — произвольное сепарабельное расширение поля K, F — некоторое алгебраическое расширение поля K, содержащееся в E. При этих условиях E сепарабельно над F* (см. § 7, n° 4).

Пусть (a_λ) — некоторый базис поля F над K, (b_μ) — некоторый базис поля E над F. Достаточно доказать, что семейство (b_μ^p) линейно свободно над F (следствие из предложения 3). Пусть $\sum_\mu \beta_\mu b_\mu^p = 0$ — линейное соотношение между элементами b_μ^p с коэффициентами $\beta_\mu \in F$. Так как элементы (a_λ^p) составляют базис поля F над K (следствие из предложения 4), имеем $\beta_\mu = \sum_{\lambda,\,\mu} \alpha_{\lambda\mu} a_\lambda^p$, где $\alpha_{\lambda\mu} \in K$. Следовательно, $\sum_{\lambda,\,\mu} \alpha_{\lambda\mu} (a_\lambda b_\mu)^p = 0$, и так как семейство $(a_\lambda b_\mu)$ образует базис поля E над K (§ 2, n° 1) (следствие из предложения 3), семейство $(a_\lambda b_\mu)^p$ линейно свободно над K, откуда следует, что $\alpha_{\lambda\mu} = 0$ для всех пар (λ, μ), т. е. $\beta_\mu = 0$ для всех μ.

4. *Радикальные расширения*

Определение 2. *Расширение $E \subset \Omega$ поля K называется радикальным, если все его элементы радикальны над K.*

Таким образом, радикальные расширения поля K суть расширения поля K, содержащиеся в $K^{p^{-\infty}}$; все они алгебраичны над K. Для любого множества A радикальных элементов над K расширение $K(A)$ радикально над K. Если E — радикальное расширение поля K, а F — радикальное расширение поля E, то F — радикальное расширение поля K, так как для всякого элемента $x \in F$ существует такое целое число m, что $x^{p^m} \in E$ и такое целое число n, что $(x^{p^m})^{p^n} \in K$, т. е. $x^{p^{m+n}} \in K$.

Предложение 6. *Для всякого радикального расширения E поля K конечной степени число $[E : K]$ является степенью характеристической экспоненты p.*

Действительно, пусть $E = K(a_1, a_2, \ldots, a_n)$ и все элементы a_i радикальны над K; тогда тем более элемент a_i радикален над полем $K(a_1, \ldots, a_{i-1})$ при $1 \leqslant i \leqslant n$, а так как число $[K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]$ является степенью p (предложение 1), число $[E : K]$ также является степенью p (§ 3, предложение 5).

ПРЕДЛОЖЕНИЕ 7. *Для любого алгебраического над K элемента $x \in \Omega$ существует такое целое число $m \geqslant 0$, что элемент x^{p^m} сепарабелен над K.*

Действительно, пусть f — минимальный многочлен элемента x; если $p = 1$, то предложение очевидно — достаточно взять $m = 0$ (§ 7, предложение 9 и § 3, предложение 1). Если $p > 0$, то пусть m — наибольшее из чисел h, для которых $f \in K[X^{p^h}]$, тогда

$$f(X) = g(X^{p^m}),$$

где $g \in K[X]$ и $g \notin K[X^p]$. Очевидно, что g — неприводимый многочлен. Так как $g \notin K[X^p]$, то все корни многочлена g простые (§ 3, предложение 1), следовательно, элемент x^{p^m}, являясь корнем многочлена g, сепарабелен над K (§ 7, предложение 9).

СЛЕДСТВИЕ. *Пусть E — алгебраическое расширение поля K, E_0 — наибольшее сепарабельное расширение поля K, содержащееся в E* (§ 7, предложение 11); *тогда E — радикальное расширение поля E_0.*

Действительно, для любого элемента $x \in E$ существует такое целое число $m \geqslant 0$, что элемент x^{p^m} сепарабелен над K (предложение 7), следовательно, $x^{p^m} \in E_0$ по определению.

ПРЕДЛОЖЕНИЕ 8. *Пусть E — алгебраическое расширение поля K, E_0 — наибольшее сепарабельное расширение K, содержащееся в E. Для того чтобы число K-изоморфизмов поля E в Ω было конечным, необходимо и достаточно, чтобы поле E_0 имело конечную степень над K; тогда это число равно $[E_0 : K]$.*

Действительно, всякий K-изоморфизм u расширения E_0 в поле Ω продолжается до некоторого K-автоморфизма поля Ω (§ 6, следствие 2 из предложения 2). Пусть v и w — K-автоморфизмы поля Ω, продолжающие u. Тогда отображение vw^{-1} является E_0-автоморфизмом поля Ω, следовательно, его ограничение на расширение E (которое радикально над E_0) будет тождественным отображением. Иначе говоря, всякий K-изоморфизм поля E_0 однозначно продолжается до K-изоморфизма поля E. Предложение вытекает тогда из сепарабельности поля E_0 (§ 7, предложение 8).

СЛЕДСТВИЕ. *Если E имеет конечную степень над K, то число K-изоморфизмов поля E в Ω является делителем степени $[E : K]$.*

Определение 3. *Пусть дано алгебраическое расширение E поля K конечной степени. Назовем сепарабельным множителем степени поля E (над K) и будем обозначать символом $[E:K]_s$ степень над K наибольшего сепарабельного расширения E_0 поля K, содержащегося в E* (равную числу K-изоморфизмов поля E в Ω); *несепарабельным множителем степени поля E (над K) называем степень поля E над E_0 и обозначаем ее $[E:K]$.*

Таким образом, число $[E:K]_i$ является степенью p (предложение 6 и следствие из предложения 7), и

$$[E:K]=[E:K]_s\,[E:K]_i.$$

Замечание. Заметим, что несепарабельный множитель степени поля E не обязательно равен наибольшей степени p, на которую делится число $[E:K]$, так как может существовать сепарабельное расширение поля K степени p (§ 11, предложение 5 и упражнение 8).

Когда степень поля E_0 над K (соответственно степень поля E над E_0) *бесконечна*, говорят еще для удобства речи, что сепарабельный множитель (соответственно несепарабельный множитель) степени поля E над K *бесконечен*.

Упражнения. *1) а) Пусть L — поле характеристики $p>0$, x и y — такие радикальные над L элементы, что $x\notin L$, $y\notin L$, $x^p\in L$, $y^p\in L$. Доказать эквивалентность условий $y\in L(x)$ и $x\in L(y)$.

б) Пусть E — расширение поля K характеристики $p>0$. Часть M расширения E назовем *p-независимой над K*, если для любой части M' множества M, отличной от M, поля $K(E^p)(M')$ и $K(E^p)(M)$ различны. Для того чтобы семейство M было p-независимо над K, необходимо и достаточно, чтобы любая ковечная часть семейства M была p-независима над K.

в) Часть M расширения E поля K назовем *p-базисом* (или *базисом несовершенства*), если семейство M p-независимо над K и если $E=K(E^p)(M)$. Пусть S — такая часть E, что $E=K(E^p)(S)$, M — часть множества S, p-независимая над K; доказать существование такого p-базиса B расширения E над K, что $M\subset B\subset S$ (см. § 5, упражнение 14).

г) Для того чтобы конечное семейство $(x_i)_{1\leqslant i\leqslant r}$ различных элементов расширения E было p-независимо над K, необходимо и достаточно, чтобы элементы $z_{\nu_1\nu_2\ldots\nu_r}=x_1^{\nu_1}x_2^{\nu_2}\ldots x_r^{\nu_r}$ $(0\leqslant\nu_i\leqslant p$ для всех $i)$ были линейно независимы над полем $K(E^p)$. В частности, для того чтобы расширение E имело p-базис из r элементов, необходимо и достаточно, чтобы выполнялось условие $[E:K(E^p)]=p^r$. Назовем *r-степенью несовершенства* поля E над K. Если $r=0$,

то есть $K(E^p)=E$, то расширение E называют *относительно совершенным* над K (например, алгебраическое и сепарабельное над K расширение E относительно совершенно над K).

*2) а) Пусть E — некоторое расширение поля K характеристики $p>0$, B — p-базис поля E над K (упражнение 1в)). Доказать, что для любого неотрицательного целого числа k $E=K(E^{p^k})(B)$.

б) Предположим, что $E\subset K^{p^{-n}}$. Для того чтобы степень $[E:K]$ была конечной, необходимо и достаточно, чтобы степень несовершенства m_0 расширения E над K (упражнение 1 г) была конечной. Таким образом, m_0 — минимальное число образующих поля E над K. Если m_k — степень несовершенства поля $K(E^{p^k})$ над K, то $m_{k+1}\leqslant m_k$ для всех k; положим $f=\sum_k m_k$; тогда $[E:K]=p^f$.

в) Предположим, что $E\subset K^{p^{-1}}$, и пусть K_0 — такое подполе поля K, что E *сепарабельно* над K_0. Доказать p-независимость семейства B^p над K_0. (Заметить, что если (a_λ) — базис поля K над K_0, то (a_λ^p) — базис поля $K_0(K^p)$ над K_0.)

Пусть C — часть поля K без общих элементов с B^p и такая, что множество $B^p\cup C$ является p-базисом поля K над K_0. Доказать, что объединение $B\cup C$ составляет p-базис поля E над K_0.

г) Опять предположим, что $E\subset K^{p^{-h}}$ и что поле E сепарабельно над подполем K_0 поля K. Доказать, что если степень несовершенства поля K над K_0 конечна, то E имеет ту же степень несовершенства, что K над K_0 (использовать в)).

*3) Пусть E — расширение поля K характеристики $p>0$, F — расширение поля E.

а) Если B — p-базис поля E над K, C — p-базис поля F над E, то существует p-базис поля F над K, содержащийся в $B\cup C$.

б) Если F — сепарабельное расширение поля E, то любые два из следующих предложений влекут третье: α) семейство B образует p-базис поля E над K; β) семейство C образует p-базис поля F над E; γ) семейство $B\cup C$ образует p-базис поля F над K и $B\cap C=\phi$ (воспользоваться тем, что если (c_μ) — базис поля F над E, то (c_μ^p) образует базис поля $K(F^p)$ над $K(E^p)$ и базис поля $E(F^p)$ над E).

*4) Пусть K — поле положительной характеристики p, E — некоторое расширение поля K и F — расширение конечного типа поля E. Доказать, что если степень несовершенства поля E над K конечна, то она не меньше степени несовершенства поля F над K (свести к двум следующим случаям: 1° F сепарабельно над E, 2° $F=E(x)$, где $x^p\in E$).

*5) Пусть K — несовершенное поле, E — алгебраическое расширение поля K конечной степени. Для того чтобы E было простым

расширением поля K, необходимо и достаточно, чтобы его степень несовершенства над K была равна 0 или 1 (для доказательства достаточности заметить, что если E_0 — наибольшее сепарабельное расширение поля K, содержащееся в E, то $[E=E_0(\alpha)$ и $E_0=K(\beta)$, и доказать, что можно найти элемент $\lambda \in K$ такой, что $E=K(\alpha+\beta\lambda)$, поскольку поле K бесконечно).

6) Пусть E — расширение конечной степени поля K. Пусть $r>0$ — степень несовершенства поля E над K; доказать, что r — наименьшее число образующих полн E над K (для того чтобы доказать, что E порождается r элементами, заметить, что если E_0 — наибольшее сепарабельное расширение поля K, содержащееся в E, то существует r элементов a_i $(1 \leqslant i \leqslant r)$ таких, что $E=E_0(a_1, \ldots, a_r)$, и использовать упражнение 5).

Вывести отсюда, что для того чтобы *всякое* алгебраическое расширение конечной степени поля K характеристики $p>0$ было простым, необходимо и достаточно, чтобы степень несовершенства поля K над K^p была равна 0 или 1.

7) Пусть F — сепарабельное расширение поля K. Если поле $E \subset F$ является относительно совершенным расширением поли K, то доказать, что F сепарабельно над E.

8) Пусть K — поле положительной характеристики $p>0$. Если E — относительно совершенное расширение поля K или алгебраическое расширение поля K, то $E^{p^{-\infty}}=E(K^{p^{-\infty}})$ (во втором случае использовать радикальность E над наибольшим сепарабельным расширением E_0 поля K, содержащимся в E).

9) Пусть K — поле положительной характеристики p, E — *сепарабельное* расширение поля K, B — p-базис поля E над K.

а) Доказать, что семейство B алгебраически свободно над K (рассмотреть алгебраическое соотношение наименьшей положительной степени между элементами B и представить степени переменных, которые в нем участвуют, в виде $kp+h$, где $0 \leqslant h \leqslant p-1$). Вывести отсюда, что если E имеет конечную алгебраическую размерность над K, то степень несовершенства E над K не превосходит алгебраической размерности E над K.

б) Доказать, что поле E сепарабельно и относительно совершенно над полем $K(B)$.

10) Назовем базис трансцендентности B расширенин E поля K *сепарабельным*, если поле E является алгебраическим сепарабельным расширением поля $K(B)$ (см. § 9, п° 3). Для того чтобы расширение E полн K положительной характеристики p и *конечной* алгебраической размерности над K допускало сепарантный базис трансцендентности над K, необходимо и достаточно, чтобы поле E было сепарабельно над K и его степень несовершенства над K была равна его алгебраической размерности над K. Таким образом, всякий p-базис полн E над K является сепарабельным базисом трансцен-

дентности поля E над K (использовать упражнение 9б) и упражнение 3б)).

11) Доказать, что относительно совершенное трансцендентное расширение E поля K положительной характеристики p не может иметь конечный тип над K. (Доказать, используя предложение 4, что в противном случае для любого базиса трансцендентности B расширения E яад K расширение E сепарабельно над $K(B)$.)

12) Пусть K — поле положительной характеристики p, E — *сепарабельное* расширение K *конечной* алгебраической размерности.

а) Если существует *некоторый* базис трансцендентности T_0 расширения E над K и неотрицательное число m такое, что $K(E^{p^m})$ сепарабельно над $K(T_0)$, то доказать, что для *любого* базиса трансцендентности T расширения E над K существует такое неотрицательное число $n \geqslant 0$, что поле $K(E^{p^n})$ сепарабельно над $K(T)$.

б) Вывести отсюда, что если выполнено условие а), то E допускает сепарантный базис трансцендентности над K (есть B есть p-базис полн E над K, S — базис трансцендентности полн E над K, содержащий B (упражнение 9а)), то, используя упражнение 9б), доказать, что S — сепарантный базис трансцендентности).

13. Пусть K — несовершенное поле характеристики p и x — элемент, трансцендентный над K. Доказать, что объединение E расширений $K(x^{p^{-n}})$ поля K является сепарабельным расширением K алгебраической размерности 1, не допускающим сепарантного базиса трансцендентности над K.

*14) Пусть E — расширение поля K, F — расширение поля E.

а) Если поле E допускает сепарантный базис трансцендентности над K и если F допускает сепарантный базис трансцендентности над K, то поле F допускает сепарантный базис трансцендентности над K.

б) Если поле F допускает сепарантный базис трансцендентности над K и если E имеет конечную алгебраическую размерность над K, то поле E допускает сепарантный базис трансцендентяости над K (свести к случаю, когда F имеет конечную алгебраическую размерность над K и применить упражнение 12).

в) Если F допускает сепарантный базис трансцендентности над K и сепарабельно над E, то поле F допускает сепарабельный базис трансцендентности над E (использовать упражнение 12).

15) Пусть K — поле положительной характеристики p и степени несовершенства над K^p, равной 1. Для того чтобы расширение E поля K было сепарабельно над K, необходимо и достаточно, чтобы поле E не содержало никакого радикального над K элемента, не принадлежащего K (если элемент a поля K образует базис поля K над K^p, то доказать, что поля $K^{p^{-1}} = K(a^{p^{-1}})$ и E линейно разделены над K).

16) Пусть f — унитарный неприводимый многочлен кольца $K[X]$, K — поле положительной характеристики p. Доказать, что в кольце $K[X]$ многочлен $f(X^p)$ неприводим или является p степенью неприводимого многочлена в зависимости от того, существует или нет коэффициент многочлена f, не принадлежащий полю K^p.

*17) Пусть K_0 — поле характеристики $p>2$, и пусть K — поле рациональных функций $K_0(X, Y)$. Рассмотрим алгебраическое расширение $E=K(\vartheta)$ поля K, порожденное корнем ϑ многочлена $f(Z)=Z^{2p}+XZ^p+Y$ в кольце $K[Z]$. Доказать, что поле E не сепарабельно над K, но не содержит радикальных над K элементов, не принадлежащих K (см. упражнение 15). (Заметить сначала, что многочлен f неприводим в кольце $K[Z]$; если существует такой элемент $\beta \in E$, что $\beta^p \in K$, $\beta \notin K$, то f приводим в кольце $K(\beta)(Z)$; используя упражнение 16, доказать, что тогда элементы $X^{1/p}$ и $Y^{1/p}$ принадлежат E и что $[E:K] \geqslant p^2$.)

18) Пусть Ω — алгебраически замкнутое расширение поля K, E и F — расширения поля K конечной алгебраической размерности, содержащиеся в Ω, и $E \subset F$. Пусть (u_α) — семейство K-автоморфизмов поля Ω таких, что ограничения u_α на E попарно различны и составляют множество K-изоморфизмов поля E в Ω. Пусть (v_β) — семейство различных E-изоморфизмов. Доказать, что всякий K-изоморфизм поля F может быть однозначно записан в виде $u_\alpha \circ v_\beta$. Вывести отсюда, что если E и F — алгебраические расширения поля K конечной степени и $E \subset F$, то $[F:K]_s=[F:E]_s[E:K]_s$.

§ 9. Дифференцирования в полях

1. *Продолжение дифференцирования*

Пусть Ω — некоторое поле, E — подполе в Ω. Мы уже определили в главе IV, § 4, n° 3 и 4 понятие *дифференцирования подполя* E в поле Ω (где поле E рассматривалось как алгебра над кольцом Z целых рациональных чисел).

Предложение 1. *Для каждого дифференцирования D подполя E в поле Ω множество N тех элементов $x \in E$, для которых $Dx=0$, является подполем поля E.*

В самом деле, известно, что N является подкольцом поля E, содержащим единицу (гл. IV, § 4, n° 3 и 4). С другой стороны, так как всякое дифференцирование в поле Ω любой области целостности, содержащейся в Ω, однозначно продолжается до дифференцирования ее поля дробей (гл. IV, § 4, предложение 11), множество N совпадает с этим полем дробей.

Отсюда следует, что $D(ax) = aDx$ для всех $a \in N$, $x \in E$; другими словами, D является дифференцированием подполя E поля Ω, если поле E рассматривать как *алгебру над полем* N. Вообще пусть K — произвольное подполе поля E; всякое дифференцирование подполя E в Ω, рассматриваемого как *алгебра над* K, называется *K-дифференцированием*. Эти дифференцирования D характеризуются тем свойством, что $Dx = 0$ для всех $x \in K$.

Из предыдущего вытекает, в частности, что всякое дифференцирование *простого* поли в любом его расширении является *нулевым*.

Предложение 2. *Пусть E — некоторое подполе поля Ω, D — дифференцирование поля E в Ω, $F = E(x_\iota)_{\iota \in I}$ — расширение поля E, содержащееся в Ω, и $(u_\iota)_{\iota \in I}$ — семейство элементов из Ω. Для того чтобы существовало дифференцирование D поля F, являющееся продолжением дифференцирования D и такое, что $\overline{D}(x_\iota) = u_\iota$ для всех $\iota \in I$, необходимо и достаточно, чтобы для каждого конечного подмножества $H \in I$ существовало дифференцирование D_H поля $E(x_\iota)_{\iota \in H}$, являющееся продолжением дифференцирования D и такое, что $D_H(x_\iota) = u_\iota$ для каждого $\iota \in H$. Дифференцирование D в этом случае является единственным.*

Единственность $\overline{D}$ следует из того, что множество тех элементов $x \in F$, которые аннулируются некоторым дифференцированием, является подполем в F: если оно содержит E и x_ι, то оно совпадает с F. Если продолжение D_H существует для каждого конечного подмножества $H \in I$, то для двух таких подмножеств $H \subset L$ дифференцирование D_L является продолжением D_H в силу единственности D_L.

Для каждого элемента $x \in F$ существует такое конечное множество H, что $x \in E(x_\iota)_{\iota \in H}$ (§ 2, следствие предложения 3), и значение $D_H(x)$ в силу сказанного выше не зависит от выбора конечного множества H, удовлетворяющего этому условию; обозначив это значение через $\overline{D}x$, мы определим, таким образом, $\overline{D}$ на всем поле F. Остается убедиться в том, что $\overline{D}$ является дифференцированием, но это немедленно следует из того, что для всяких двух элементов x и y, принадлежащих F, существует такое конечное множество $H \in I$, что x и $y \in E(x_\iota)_{\iota \in H}$.

В частности, *нулевое* дифференцирование является единственным дифференцированием поля F, аннулирующим все поле E и каждый из элементов x_ι.

Предложение 3. *Пусть E — некоторое подполе поля Ω, D — дифференцирование подполя E в Ω. Пусть $F = E(x_1, \ldots, x_n)$ — расширение конечного типа поля E, лежащее в Ω, $\mathfrak{a}$ — идеал алгебраических соотношений между элементами x_i с коэффициентами из E* (множество таких многочленов $f \in E[X_1, \ldots, X_n]$, что $f(x_1, \ldots, x_n) = 0$). *Для данного семейства u_i $(1 \leqslant i \leqslant n)$ элементов поля Ω необходимым и достаточным условием существования дифференцирования $\overline{D}$ поля F в Ω, являющегося продолжением дифференцирования D и такого, что $\overline{D}x_i = u_i$ для всех $1 \leqslant i \leqslant n$, является выполнение равенств*

$$f^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} u_i = 0, \tag{1}$$

где f^D — многочлен (кольца $\Omega[X_i, \ldots, X_n]$), полученный применением дифференцирования D к каждому коэффициенту многочлена f (гл. IV, § 4, n° 4).

Покажем сначала, что условия (1) необходимы и достаточны для того, чтобы можно было продолжить дифференцирование D до дифференцирования $\overline{D}$ кольца $E[x_1, x_2, \ldots, x_n]$, удовлетворяющего условиям $\overline{D}x_i = u_i$ $(1 \leqslant i \leqslant n)$. Каждый элемент из $E[x_1, \ldots, x_n]$ имеет вид $g(x_1, \ldots, x_n)$, где $g \in E[X_1, X_2, \ldots, X_n]$.

В силу правила вычисления производной для каждого дифференцирования $\overline{D}$, являющегося продолжением D, имеет место тождество

$$\overline{D}(g(x_1, \ldots, x_n)) = g^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i} u_i, \tag{2}$$

откуда сразу же следует необходимость условий (1). Обратно, если эти условия выполнены, то для каждого элемента $y = g(x_1, \ldots, x_n)$ из $E[x_1, \ldots, x_n]$ мы можем определить $\overline{D}y$ с помощью правой части равенства (2), так как условие (1) показывает, что определенное таким образом значение $\overline{D}y$ будет одним и тем же для каждого многочлена g такого, что $y = g(x_1, \ldots, x_n)$. Нетрудно убедиться, что описанное отобра-

жение $\overline{D}$ является дифференцированием кольца $E[x_1, \ldots, x_n]$, удовлетворяющим нужным условиям; оно однозначно продолжается на поле дробей $E(x_1, \ldots, x_n)$ кольца $E[x_1, \ldots, x_n]$ (гл. IV, § 4, предложение 11), чем и завершается доказательство.

Замечание. Пусть (f_λ) — некоторая система образующих идеала $\mathfrak{a}$; для того чтобы условие (1) выполнялось для каждого многочлена $f \in \mathfrak{a}$, достаточно, чтобы оно выполнялось для всех f_λ.

В самом деле, каждый многочлен $f \in \mathfrak{a}$ записывается, по предположению, в виде $f = \sum_\lambda \varphi_\lambda f_\lambda$, где φ_λ — некоторые многочлены; следовательно,

$$f^D = \sum_\lambda \varphi_\lambda^D f_\lambda + \sum_\lambda \varphi_\lambda f_\lambda^D \text{ и } \frac{\partial f}{\partial x_i} = \sum_\lambda \frac{\partial \varphi_\lambda}{\partial x_i} f_\lambda + \sum_\lambda \frac{\partial f_\lambda}{\partial x_i}.$$

Так как, согласно предположению, $f_\lambda(x_1, \ldots, x_n) = 0$ для всех λ, имеем

$$f^{\overline{D}}(x_1, \ldots, x_n) + \sum_i \frac{\partial f}{\partial x_i} u_i = \sum_\lambda \varphi_\lambda(x_1, \ldots, x_n) \left(f_\lambda^D(x_1, \ldots, x_n) + \sum_{i=1}^n \frac{\partial f_\lambda}{\partial x_i} u_i \right),$$

откуда следует наше утверждение.

Применим критерий предложения 3 к различным типам расширений полей.

Предложение 4. Пусть $F \subset \Omega$ — *чисто трансцендентное расширение поля* E, (x_ι) *чистый базис поля* F *над* E.

Для каждого дифференцирования D *поля* E *в* Ω *и каждого семейства* (u_ι) *элементов из* Ω *существует дифференцирование* $\overline{D}$ *поля* F *в* Ω, *причем единственное, продолжающее* D *и такое, что* $\overline{D}x_\iota = u_\iota$ *для каждого* ι.

В самом деле, идеал $\mathfrak{a}$ алгебраических соотношений между элементами x_ι с коэффициентами из поля E сводится к нулю, следовательно, условия (1) выполняются.

Предложение 5. *Если* $F \subset \Omega$ — *сепарабельное алгебраическое расширение поля* E, *то каждое дифференцирование* D *поля* E *в* Ω *однозначно продолжается до дифференцирования* $\overline{D}$ *поля* E *в* Ω.

Сначала покажем, что если продолжение возможно, то оно единственно. В самом деле, пусть $f \in E[X]$ — минимальный

многочлен некоторого элемента $x \in F$ над полем E; в силу формулы (1) должно выполняться равенство $f^D(x) + f'(x)\overline{D}x = 0$; поскольку элемент x сепарабелен над E, $f'(x) \neq 0$ (§ 7, предложение 9), так что элемент $\overline{D}x$ определен однозначно.

Для доказательства существования $\overline{D}$ достаточно рассмотреть тот случай, когда поле $F = E(x_1, \ldots, x_n)$ является конечным расширением над E (предложение 2). Проведем индукцию по n; при $n = 0$ утверждение очевидно. Положим $L = E(x_1, x_2, \ldots, x_{n-1})$; тогда $F = L(x_n)$ и элемент x_n сепарабелен над L (§ 7, следствие 3 предложения 9). По предположению, дифференцирование D_1 поля L является продолжением D. Пусть g — минимальный многочлен элемента x_n над L; для существования дифференцирования $\overline{D}$ поля F, продолжающего D_1, в силу замечания к предложению 3, необходимо и достаточно, чтобы можно было так определить значение $\overline{D}x_n$ в Ω, чтобы оно удовлетворяло уравнению

$$g^{D_1}(x_n) + g'(x_n)\,\overline{D}x_n = 0,$$

а это всегда возможно, поскольку $g'(x_n) \neq 0$.

Следствие 1. *Пусть D — такое дифференцирование поля E, что $D(E) \subset E$; тогда $\overline{D}(F) \subset F$.*

Следствие 2. *Любое K-дифференцирование расширения E поля K является нулевым в каждом алгебраическом сепарабельном расширении поля K, содержащемся в E.*

В частности, так как каждое дифференцирование *простого* поля P является нулевым и так как P совершенно (§ 7, следствие предложения 5), каждое дифференцирование *алгебраического* расширения поля P нулевое.

Предложение 6. *Пусть $E \subset \Omega$ — радикальное расширение поля K конечной степени, большей* 1; *тогда существует ненулевое K-дифференцирование поля E в Ω.*

В самом деле, пусть $(x_i)_{1 \leqslant i \leqslant n}$ — система образующих поля E над K такая, что $x_n \notin K(x_1, \ldots, x_{n-1})$, элемент x_n радикален над L; пусть $f(X) = X^{p^e} - a$ — его минимальный над L многочлен (где p — характеристика Ω). Для того чтобы K-дифференцирование D поля L продолжалось до дифференцирования $\overline{D}$ поля E, необходимо и достаточно, чтобы $\overline{D}x_n$ можно было определить

из соотношения $f^D(x_n)+f'(x_n)\overline{D}(x_n)=0$. Это означает, что $f^D(x_n)=0$, что, вообще говоря, не всегда верно; но для $D=0$, очевидно, $f^D(x_n)=0$ и, следовательно, существует такое K-дифференцирование $\overline{D}$ поля E, что $\overline{D}x_n$ — произвольный элемент из Ω.

2. *Дифференцирования сепарабельных расширений*

Теорема 1. *Для того чтобы конечное расширение $E\subset\Omega$ поля K было алгебраическим и сепарабельным над K, необходимо и достаточно, чтобы единственным K-дифференцированием поля E в Ω было нулевое дифференцирование.*

Условие необходимо в силу следствия 2 предложения 5. Обратно, пусть $E=K(x_1, x_2, \ldots, x_n)$ — конечное расширение поля K; положим $E_0=K$, $E_i=K(x_1, x_2, \ldots, x_i)$ для $1\leqslant i\leqslant n$. Пусть h — наименьшее целое i, для которого поле $E=E_n$ алгебраично и сепарабельно над E_i; мы хотим доказать, что число h не может быть положительным. В противном случае поле $E_h=E_{h-1}(x_h)$ не было бы алгебраическим и сепарабельным над E_{h-1} (§ 7, предложение 7). Если элемент x_h трансцендентен над E_{h-1}, то существует ненулевое на E_h K-дифференцирование D (предложение 4). Если же элемент x_h алгебраичен над E_{h-1}, то он не сепарабелен над E_{h-1}. Пусть F — наибольшее алгебраическое сепарабельное расширение поля E_{h-1}, содержащееся в E_h; по предположению, $F\neq E_h$ и E_h — радикальное расширение поля F (§ 8, предложение 7); следовательно, существует K-дифференцирование D, ненулевое на E_h (предложение 6). В обоих случаях дифференцирование D продолжается на $E=E_h$ (предложение 5), что завершает доказательство.

Если E не является расширением конечного типа поля K, может случиться, что нулевое дифференцирование по-прежнему является единственным K-дифференцированием, но поле E уже не сепарабельно над K. Например, пусть K — несовершенное поле характеристики p; тогда каждое K-дифференцирование D поля $E=K^{p^{-\infty}}$ является нулевым, так как для каждого элемента $x\in E$ существует элемент $y\in K$ такой, что $x=y^p$, следовательно, $Dx=py^{p-1}Dy=0$.

Следствие. *Пусть f_i $(1\leqslant i\leqslant n)$ суть n многочленов из $K[x_1, \ldots, x_n]$; x_i $(1\leqslant i\leqslant n)$ — такие n элементов поля Ω,*

что $f_i(x_1, \ldots, x_n) = 0$ *для всех* $1 \leqslant i \leqslant n$. *Если определитель* $\det\left(\frac{\partial f_i}{\partial x_j}\right)$ *не равен нулю, то поле* $K(x_1, \ldots, x_n)$ *является алгебраическим и сепарабельным расширением поля* K.

В самом деле, пусть D — какое-нибудь K-дифференцирование поля $K(x_1, \ldots, x_n)$; из n соотношений $f_i(x_1, \ldots, x_n) = 0$ следует (гл. IV, § 4, предложение 9), что

$$\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j} Dx_j = 0 \quad (1 \leqslant i \leqslant n),$$

откуда, в силу предположения, $Dx_j = 0$ для $1 \leqslant j \leqslant n$, а это означает, что $D = 0$ (предложение 2).

3. *Сепарабельные базисы трансцендентности*

Пусть Ω — некоторое расширение поля K, E — подрасширение поля Ω; обозначим символом Ω_K множество Ω, наделенное структурой векторного пространства над полем K. K-дифференцирования поля E в Ω являются частичными линейными отображениями поля E в Ω_K; отсюда немедленно следует, что они образуют векторное подпространство над Ω векторного пространства $\mathscr{L}(E, \Omega_K)$ (см. § 7, n° 1).

Теорема 2. *Пусть* $E = K(x_1, x_2, \ldots, x_n) \subset \Omega$ — *сепарабельное расширение конечного типа поля* K. *Пусть* r — *алгебраическая размерность поля* E *над полем* K; *тогда векторное пространство* $\mathscr{D}$ (*над* Ω) K-*дифференцирований поля* E *в* Ω *имеет ту же размерность* r, *существует часть* B *множества элементов* x_i *такая, что* B *является базисом трансцендентности поля* E *над* K *и* E *является алгебраическим сепарабельным расширением поля* $K(B)$.

Пространство $\mathscr{D}$ имеет конечную размерность $\leqslant n$. В самом деле, пусть D_K $(1 \leqslant K \leqslant n+1)$ — система $(n+1)$ K-дифференцирований поля E в Ω; существует $n+1$ элементов a_i $(1 \leqslant i \leqslant n+1)$ поля Ω, среди которых не все равны нулю, с условием $\sum_{i=1}^{n+1} a_i D_i x_j = 0$ при $1 \leqslant j \leqslant n$; поэтому $\sum_{i=1}^{n+1} a_i D_i = 0$ (предложение 2). Пусть теперь $s \leqslant n$ — размерность пространства $\mathscr{D}$ и $(D_i)_{1 \leqslant i \leqslant s}$ — базис пространства $\mathscr{D}$ (над Ω). Матрица $(D_i x_j)$ из s строк и n

столбцов имеет ранг s, ибо иначе предыдущие рассуждения показали бы, что дифференцирования D_i над Ω линейно зависимы. Сделав, если нужно, перестановку x_j, можно, следовательно, считать, что определитель $\det(D_i x_j)$, где $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant s$ не равен нулю (гл. III, § 7, предложение 1). Покажем в первую очередь, что поле E *алгебраично* и *сепарабельно* над полем $F(x_1, x_2, \ldots, x_s)$; в самом деле, если D — F-дифференцирование поля E, то D является тем более K-дифференцированием поля E; следовательно, $D = \sum_{i=1}^{s} a_i D_i$, где $a_i \in \Omega$; а так как $Dx_j = 0$ для $1 \leqslant j \leqslant s$, иными словами, $\sum_{i=1}^{s} a_i D_i x_j = 0$ для $1 \leqslant j \leqslant s$, то $a_i = 0$, $1 \leqslant i \leqslant s$, т. е. $D = 0$, что в силу теоремы 1 доказывает наше утверждение.

Остается установить *алгебраическую независимость* над K элементов $x_1, x_2, \ldots, x_s$. Пусть $\mathfrak{a}$ — идеал алгебраических соотношений между элементами $x_1, x_2, \ldots, x_s$ над полем K, и пусть $\mathfrak{a} \neq 0$. Пусть $f \neq 0$ — многочлен *наименьшей* (общей) степени в $\mathfrak{a}$; тогда $f(x_1, \ldots, x_s) = 0$, следовательно (гл. IV, § 4, предложение 9), $\sum_{j=1}^{s} \frac{\partial f}{\partial x_j} D_i x_j = 0$ для $1 \leqslant i \leqslant s$ и, значит, $\frac{\partial f}{\partial x_j} = 0$ для $1 \leqslant j \leqslant s$; иначе говоря, $\frac{\partial f}{\partial x_j} \in \mathfrak{a}$ для всех $1 \leqslant j \leqslant s$; в силу выбора f отсюда следует, что $\frac{\partial f}{\partial x_j} = 0$ для $1 \leqslant j \leqslant s$. Если поле K имеет характеристику нуль, то f необходимо является константой $\neq 0$, что невозможно, следовательно, $\mathfrak{a} = (0)$.

Если поле K имеет характеристику $p > 0$, f принадлежит кольцу $K[X_1^p, \ldots, X_s^p]$ (§ 1, предложение 4); другими словами, $f = \sum_{\lambda} c_\lambda Z_\lambda^p$, где $c_\lambda \in K$ и где Z_λ — многочлены от X_i $(1 \leqslant i \leqslant s)$. Поскольку поле E сепарабельно над K, в силу критерия Маклейна (§ 8, следствие предложения 3) существуют элементы $d_\lambda \in K$, не все равные нулю, такие, что многочлен $g = \sum_{\lambda} d_\lambda Z_\lambda$ также принадлежит идеалу $\mathfrak{a}$, а это противоречит выбору f. Следовательно, мы снова приходим к абсурдному заключению, и в этом случае также показано, что $\mathfrak{a} = (0)$. Доказательство закончено.

Базис трансцендентности B поля E над полем K, для которого поле E является (алгебраическим) сепарабельным расширением поля $K(B)$, называется *сепарабельным базисом трансцендентности* поля E над K. Заметим, что если E обладает сепарабельным базисом трансцендентности B над K, то другой базис трансцендентности B' поля E над K не обязан быть сепарабельным: например, если поле K имеет характеристику $p>0$ и поле $E=K(X)$ сепарабельно над K (§ 7, предложение 3), то X образует сепарабельный базис трансцендентности поля E над K, но X^p также образует базис трансцендентности поля E над K, а поле E является радикальным расширением поля $K(X^p)$. Отметим также, что сепарабельное расширение E поля K, не являющееся конечным над K, может не иметь ни одного сепарантного базиса трансцендентности (§ 8, упражнение 13).

Предложение 7. *Пусть E и F — два расширения поля K, алгебраически разделенные над K, и пусть F сепарабельно над K; тогда поле $E(F)$ сепарабельно над E.*

Достаточно показать, что для каждой конечной части $M \subset F$ поле $E(M)$ сепарабельно над E (§ 7, предложение 6). Положим $L=K(M)$, тогда $E(M)=E(L)$, следовательно, можно ограничиться случаем, когда поле F конечного типа над K.

Пусть B — сепарабельный базис трансцендентности поля F над K (теорема 2); так как, по предположению, семейство B алгебраически свободно над E (§ 5, предложение 9), поле $E(B)$ является чистым расширением поля E, и следовательно, сепарабельно над E (§ 7, предложение 3). Поскольку каждый элемент поля F алгебраичен и сепарабелен над $K(B)$, он тем более алгебраичен и сепарабелен над $E(B)$ (§ 7, следствие 3 предложения 9); значит, расширение $E(F)$ сепарабельно над $E(B)$ и, следовательно (§ 7, предложение 7), над E.

Напротив, если не предполагать, что расширения E и F алгебраически разделены над K, поле $E(F)$ может не быть сепарабельным над E даже в случае, когда F сепарабельно над K.

Например, пусть x — трансцендентный над K элемент, a — радикальный над K элемент, не принадлежащий полю K; тогда элемент $(x+a)$ трансцендентен над K, поэтому поля $E=K(x)$ и $F=K(x+a)$ являются чистыми трансцендентными расширениями поля K и, следовательно, сепарабельны над K.

Но поле $E(F)$ содержит элемент $a=x+a-x$, радикальный над E и не принадлежащий E, поскольку поле $K(a)$ не сепарабельно над K.

Следствие. *Пусть E и F — два сепарабельных расширения поля K, алгебраически разделенные над K, тогда поле $K(E \cup F)$ сепарабельно над K.*

В самом деле, в силу предложения 7 поле $K(E \cup F)$ сепарабельно над E, откуда следует утверждение, так как поле E сепарабельно над K (§ 7, предложение 7).

Упражнения. 1) Пусть K — поле характеристики $p > 0$, Ω — некоторое расширение поля K, E — подрасширеяие поля Ω. Показать, что каждое K-дифференцирование поля E в Ω является нулевым в поле $K(E^p)$. Пусть B — любой p-базис поля E над K (§ 8, упражнение 1); для каждого элемента $x \in B$ существует такое K-дифферея-цирование D поля E, что $Dx = 1$ и $Dy = 0$ для всех $y \in B$, $y \neq x$; в частности, если степень несовершенства поля E над K (§ 8, упражнение 1) конечна, то размерность (над Ω) пространства K-дифференцирований поля E равна этой степени.

Вывести из этих результатов, что если F — сепарабельное расширение поля E, то каждое K-дифференцирование поля E можно продолжить до некоторого K-дифференцирования всего поля F (использовать упражнение 3б) из § 8).

* 2) Пусть K — поле характеристики $p > 0$, Ω — расширение поля K, E и F — подрасширения поля Ω, алгебраически разделеяные над K. Пусть L — наибольшее алгебраическое и сепарабельное расширение поля K, содержащееся в F; показать, что $E(L)$ — наибольшее алгебраическое и сепарабельное расширение полн E, содержащееся в $E(F)$. (Свести к случаю, когда $L = K$; пусть B — базис трансцендентности поля E над K и H — алгебраическое замыкание полн K в F; используя упражнение 8д) § 6, показать, что $H(B)$ — алгебраическое замыкание поля $K(B)$ в поле $F(B)$, радикальное над $K(B)$. Показать затем, что для всякого алгебраического над E элемента $x \in E(F)$ существует целое число $r \geqslant 0$ и конечное число элементов $u_i \in E$ $(1 \leqslant i \leqslant n)$ таких, что элемент $x^{p^r} = y$ принадлежит алгебраическому сепарабельному расширению $M = F(B)(u_1, \ldots, u_n)$ поля $F(B)$, причем u_i образуют базис поля M над $F(B)_n$; показать, наконец, используя предложение 3 § 6, что если $y = \sum_{i=1}^{n} b_i u_i$, где $b_i \in F(b)$, то $b_i \in H(B)$, и вывести отсюда, что существует такое целое число $s \geqslant 0$, что $y^{p^s} \in E$.)

* 3) Пусть K_0 — поле характеристики $p > 0$, $K = K_0(X, Y)$ — поле рациональных дробей от двух переменных над K_0.

а) Пусть $E = K(U, u)$, где U — независимая переменная над K, а u — алгебраический над $K(U)$ элемент, определенный равенством $u^p = X + YU^p$. Показать, что поле E не сепарабельно над K, но поле K алгебраически замкнуто в поле E. (Показать, что для любого

алгебраического над K элемента $x \in E$, $x^p \in K$; если бы $x \notin K$, то $K(U, x) = K(U, u)$; вывести отсюда, используя теорему 1, что элементы $X^{1/p}$ и $Y^{1/p}$ принадлежали бы полю $K(x)$.)

б) Пусть $F = K(V, v)$, где V — друган независимая над K переменная и $v^p = X + YV^p$. Показать, что поля E и F линейно разделены над K, но что поле K не является алгебраически замкнутым в поле $K(E \cup F)$. (Показать, что $X^{1/p} \in K(E \cup F)$, вывести из этого, что элемент v не может принадлежать полю $E(V)$, заключить на основании этого, что поля E и F линейно разделены над полем K.)

4) Пусть E и F — два трансцендентных расширения поля K, линейно разделенных над K. Показать, что поле $K(E \cup F)$ отлично от кольца C (изоморфного произведению $E \otimes F$), порожденного множеством $E \cup F$. (Свести к случаю, когда поля E и F имеют алгебраическую размерность единица над полем K; если $x \in E$ и $y \in F$ — трансцендентные над K элементы, показать, что элемент $1/x+y$ не может принадлежать кольцу C; методом от противного показать, что иначе существует такое целое число $r \geqslant 0$, что элемент $1/(x+y)^{p^r}$ принадлежит подкольцу кольца C (изоморфному $K(x) \otimes K(y)$), порожденному множеством $K(x) \cup K(y)$, причем p — характеристическая экспонента поля K.)

§ 10. Расширения Галуа

1. *Определение расширений Галуа*

Определение 1. *Расширение E поля K называется расширением Галуа (над K), если оно алгебраично и если K совпадает с полем инвариантов группы всех K-автоморфизмов поля E; эта группа тогда называется группой Галуа поля E (над K).*

Пусть E — произвольное алгебраическое расширение поля K и $F \supset K$ — поле инвариантов группы всех K-автоморфизмов поля E. Поскольку каждый K-автоморфизм поля E является также F-автоморфизмом, E является расширением Галуа поля F.

Предложение 1. *Для того чтобы алгебраическое расширение E поля K было расширением Галуа, необходимо и достаточно, чтобы оно было нормальным и сепарабельным.*

Это все равно, что сказать, что *все корни минимального многочлена над K для каждого элемента $x \in E$ должны быть простыми и содержаться в E* (§ 6, определение 2 и § 7, предложения 9 и 10).

Условие *необходимо*. В самом деле, пусть x принадлежит расширению Галуа E поля K, и пусть x_i $(1 \leqslant i \leqslant n)$ — все различные сопряженные с x элементы, лежащие в E; каждый K-автоморфизм u поля E переставляет между собой элементы x_i (§ 6, определение 1), поэтому $\prod_{i=1}^{n}(X-x_i)=\prod_{i=1}^{n}(X-u(x_i))$; это доказывает, что коэффициенты многочлена $g(X)=\prod_{i=1}^{n}(X-x_i)\in E[X]$ инвариантны при всех K-автоморфизмах поля E, а тогда, согласно предположению, они принадлежат полю K. Поскольку $g(X)=0$, многочлен g кратен минимальному многочлену f элемента x над K (§ 3, теорема 1), а так как его степень не больше степени f, то $g=f$; это показывает, что все корни многочлена f просты и содержатся в E.

Условие *достаточно*. В самом деле, предположим, что оно выполнено, и пусть элемент $x\in E$ не принадлежит K; так как степень минимального многочлена f элемента x над K больше единицы и все его корни простые в E, то существует по крайней мере один элемент $y\in E$, сопряженный с x и отличный от него, следовательно (§ 6, предложение 7), существует такой K-автоморфизм u поля E, что $u(x)=y$; тем самым все доказано.

Следствие. *Каждое расширение Галуа N поля K является объединением всех подрасширений Галуа расширения N конечной степени над K.*

В самом деле, каждое нормальное подрасширение расширения N сепарабельно над K (§ 7, предложение 6), т. е. является расширением Галуа поля K, и утверждение следует из аналогичного результата (§ 6, следствие 2 предложения 9), относящегося к нормальным расширениям.

2. *Подрасширения расширения Галуа*

Предложение 2. *Пусть N — расширение Галуа поля K. Для каждого промежуточного поля E, лежащего между K и N, N является расширением Галуа поля E, и группа Галуа поля N над полем E является подгруппой группы Галуа поля N над полем K.*

В самом деле, все корни минимального многочлена f над K для каждого элемента $x \in N$ просты и содержатся в N, следовательно, то же самое справедливо для корней минимального над E многочлена элемента x, делящего многочлен f (§ 3, предложение 2), что доказывает первое утверждение предложения 2. Второе же утверждение очевидно, поскольку группу Галуа поля N над E можно отождествить с группой автоморфизмов поля N, оставляющих инвариантными элементы из E.

Предложение 3. *Пусть N — расширение Галуа поля K, и пусть Γ — его группа Галуа. Для каждого промежуточного поля E, лежащего между K и N, и каждого K-автоморфизма $\sigma \in \Gamma$ поля N поле $\sigma(E)$, сопряженное с полем E (над K), содержится в N, и группа Галуа поля N над $\sigma(E)$ совпадает с группой $\sigma \Delta \sigma^{-1}$, сопряженной с группой Галуа Δ поля N над E.*

В самом деле, для всякого $\tau \in \Gamma$ соотношение $\tau\sigma(x) = \sigma(x)$ эквивалентно равенству $\sigma^{-1}\tau\sigma(x) = x$.

Предложение 4. *Пусть N — расширение Галуа поля K, и пусть Γ — его группа Галуа. Для того чтобы промежуточное поле E, лежащее между K и N, являлось расширением Галуа поля K, необходимо и достаточно, чтобы группа Галуа Δ поля N над E была отличной от Γ подгруппой в Γ; тогда группа Галуа поля E над K изоморфна Γ/Δ.*

Для того чтобы поле E было расширением Галуа над K, необходимо и достаточно, чтобы оно было нормальным, поскольку оно сепарабельно над K (§ 7, предложение 6). Другими словами, необходимо и достаточно, чтобы $\sigma(E) = E$ *для любого автоморфизма* $\sigma \in \Gamma$ (§ 6, предложение 7). В силу предложения 3 из этого условия следует, что $\sigma \Delta \sigma^{-1} = \Delta$ для любого автоморфизма $\sigma \in \Gamma$. Обратно, так как поле $\sigma(E)$ является полем инвариантов группы $\sigma \Delta \sigma^{-1}$, из равенства $\sigma \Delta \sigma^{-1} = \Delta$ следует, что $\sigma(E) = E$, что доказывает первую часть предложения 4.

Если E — расширение Галуа над K, то для каждого $\sigma \in \Gamma$ ограничение σ_E автоморфизма σ на поле E является K-автоморфизмом поля E; отображение $\sigma \to \sigma_E$ будет представлением группы Γ *на* группу Галуа поля E (над K), поскольку каждый K-автоморфизм поля E продолжается до некоторого K-автоморфизма поля N (§ 6, предложение 7); для того чтобы σ_E было тождест-

венным отображением, необходимо и достаточно, по определению, чтобы $\sigma \in \Delta$. Тем самым утверждение доказано.

Расширение N поля K называется *абелевым*, если оно является расширением Галуа и если его группа Галуа *абелева*. Из предложения 4, в частности, вытекает следующее утверждение:

Следствие. *Если N — абелево расширение поля K, то каждое промежуточное поле, лежащее между K и N, является абелевым расширением поля K.*

3. Семейства расширений Галуа

В этом и следующих пунктах Ω означает алгебраически замкнутое расширение поля K, и все расширения поля K, которые здесь рассматриваются, являются подрасширениями расширения Ω.

Предложение 5. *Пусть (N_ι) — некоторое семейство расширений Галуа поля K. Пересечение $\bigcap_\iota N_\iota$ и поле $K(\bigcup_\iota N_\iota)$, порожденное объединением полей N_ι являются расширениями Галуа поля K.*

Действительно, каждое подрасширение сепарабельного расширения сепарабельно (§ 7, предложение 6), поэтому каждое расширение, порожденное алгебраическими элементами, сепарабельно (§ 7, предложение 10). Тогда предложение 5 является следствием аналогичного предложения для нормальных расширений (§ 6, предложение 8), если принять во внимание характеризацию расширений Галуа, данную в предложении 1.

Следствие. *Пусть (N_ι) — семейство абелевых расширений поля K*; тогда поле $N = K(\bigcup_\iota N_\iota)$, *порожденное объединением полей N_ι, также является абелевым расширением поля K.*

В самом деле, N — расширение Галуа поля K; пусть σ и τ — какие-нибудь K-автоморфизмы поля N. Для каждого ι ограничения автоморфизмов σ и τ на N_ι являются K-автоморфизмами поля N_ι (§ 6, предложение 7), а так как N_ι абелево над K, то ограничение автоморфизма $\sigma\tau\sigma^{-1}\tau^{-1}$ на N_ι является тождественным отображением. Отсюда следует (§ 6, n° 1), что $\sigma\tau\sigma^{-1}\tau^{-1}$ — тождественное отображение на всем поле $N = K(\bigcup_\iota N_\iota)$, а это означает, что N — абелево расширение поля K.

В частности, поле, порожденное объединением *всех* абелевых расширений поля K, содержащихся в Ω, является *наибольшим* абелевым расширением, содержащимся в Ω; это поле называется *абелевым замыканием* поля K. Ясно, что это расширение не зависит (с точностью до K-изоморфизма) от рассматриваемого алгебраически замкнутого расширения Ω поля K.

Предложение 6. *Пусть A — множество алгебраических над K элементов поля Ω. Для того чтобы нормальное расширение поля K, порожденное множеством $K(A)$, было расширением Галуа, необходимо и достаточно, чтобы все элементы в A были сепарабельны над K.*

Условие, очевидно, необходимо (предложение 1). Оно достаточно, поскольку элемент, сопряженный с алгебраическим сепарабельным элементом, сепарабелен (§ 7, следствие 1 предложения 9), а нормальное расширение, порожденное множеством $K(A)$, порождается множеством элементов, сопряженных с элементами из A (§ 6, предложение 9) и поскольку, наконец, каждое расширение, порожденное множеством алгебраических сепарабельных элементов, сепарабельно (§ 7, предложение 10).

Следствие. *Пусть (f_ι) — некоторое семейство сепарабельных многочленов кольца $K[X]$, A — множество их корней в Ω; тогда $K(A)$ — расширение Галуа поля K.*

В частности, *поле корней сепарабельного многочлена $f \in K[X]$* есть *расширение Галуа* поля K. Группа Галуа Γ этого расширения называется *группой Галуа многочлена f*. Пусть x_i $(1 \leqslant i \leqslant n)$ — различные корни многочлена f в Ω, и $N = K(x_1, \ldots, x_n)$ — поле корней многочлена f; ограничение каждого K-автоморфизма u поля N на множество $\{x_1, x_2, \ldots, x_n\}$ является перестановкой этого множества, и обратно, если известны значения $u(x_i)$ $(1 \leqslant i \leqslant n)$, то значение $u(x)$ определено для каждого элемента $x \in N$ (§ 6, n° 2). Следовательно, группа Галуа Γ поля N над K *канонически изоморфна* группе перестановок элементов x_i, порожденной ограничениями автоморфизмов $u \in T$ на множество элементов x_i; следовательно, Γ изоморфна *подгруппе симметрической группы* $\mathfrak{S}_n$ (но, вообще говоря, не изоморфна всей группе $\mathfrak{S}_n$; другими словами, произвольная подстановка элементов x_i не является, вообще говоря, ограничением какого-нибудь K-автоморфизма поля N).

Если f — неприводимый сепарабельный многочлен, а поле $K(x_1, x_2, \ldots, x_n)$ многочлена f совпадает с каким-либо из полей $K(x_i)$, уравнение $f(x)=0$ называется уравнением Галуа (см. § 6, n° 3). Это, в частности, будет тогда, когда поле корней $K(x_1, x_2, \ldots, x_n)$ многочлена f является абелевым расширением поля K: действительно, из следствия предложения 4 вытекает тогда, что $K(x_i)$ — абелево расширение поля K; оно содержит поэтому каждый сопряженный с x_i элемент и, следовательно, совпадает с $K(x_1, x_2, \ldots, x_n)$. В этом случае уравнение $f(x)=0$ называют *абелевым*.

4. Композит расширения Галуа и произвольного расширения

Теорема 1. *Пусть N — расширение Галуа поля K, E — какое-либо расширение поля K (содержащееся в Ω), и $L=E\cap N$. Поля E и N линейно разделены над L; $E(N)$ — некоторое расширение Галуа поля E, и каждый L-автоморфизм поля N единственным образом продолжается до E-автоморфизма поля $E(N)$; если Γ — группа Галуа поля N над L, Γ' — группа Галуа поля $E(N)$ над E, то отображение, ставящее в соответствие каждому L-автоморфизму поля N единственный E-автоморфизм поля $E(N)$, являющийся его продолжением, есть изоморфизм групп Γ и Γ'.*

Пусть u есть E-изоморфизм поля $E(N)$ в Ω, имеем

$$u(E(N))=E(u(N))=E(N),$$

поскольку $u(N)=N$,

$$\begin{array}{ccc} & N & \longrightarrow E(N) \\ & \uparrow & \uparrow \\ K & \longrightarrow L & \longrightarrow E \end{array}$$

Рис. 3.

следовательно, $E(N)$ — нормальное расширение поля E. С другой стороны, каждый элемент поля N алгебраичен и сепарабелен над K, а значит и над E (§ 7, следствие 3 предложения 9); отсюда следует, что поле $E(N)$ сепарабельно над E (§ 7, предложение 10) и поэтому является расширением Галуа поля E (предложение 1). Чтобы показать, что E и N линейно разделены над L, рассмотрим (линейный) базис (b_λ) поля E над L и покажем, что он (линейно) свободен над N (§ 2, n° 3). Рассуждаем от противного: если бы семейство (b_λ) не было свободным над N, то

существовало бы первичное *соотношение* $\sum_\lambda a_\lambda b_\lambda = 0$ между элементами b_λ с коэффициентами $a_\lambda \in N$ (гл. II, § 5, n° 4). Для любого E-автоморфизма u поля $E(N)$ тогда $\sum_\lambda u(a_\lambda)\, u(b_\lambda) = 0$, т. е. $\sum_\lambda u(a_\lambda)\, b_\lambda = 0$. Но $u(a_\lambda) \in N$, следовательно, существует такой элемент $\varrho \in N$, что $u(a_\lambda) = \varrho a_\lambda$ для всех λ (гл. II, § 5, предложение 2), а так как существует такой индекс μ, что $a_\mu = 1$, то $\varrho = 1$. Это означает, что все коэффициенты a_λ инвариантны при каждом E-автоморфизме поля $E(N)$ и поэтому (определение 1) принадлежат E, что противоречит предположению.

Заметим теперь, что поле $E(N)$ как расширение L изоморфно тензорному произведению $E \otimes N$ (§ 3, предложение 7 и § 2, n° 3); поле $E(N)$, рассматриваемое как расширение поля E, совпадает тогда с алгеброй, полученной при помощи расширения до E поля операторов L алгебры N (гл. III, § 3, n° 4). Следовательно, каждый L-автоморфизм поля N однозначно продолжается до некоторого E-эндоморфизма поля $E(N)$ (гл. III, § 3, предложение 5), а каждый E-эндоморфизм поля $E(N)$ является автоморфизмом (§ 6, предложение 4). Тем самым теорема доказана.

Следствие 1. *Для каждого поля F, промежуточного между E и $E(N)$, справедливо равенство $F = E(F \cap N)$.*

Действительно, $E(N)$ — расширение Галуа над F (предложение 2). Пусть Δ' — группа Галуа поля $E(N)$ над F; в силу теоремы 1 она изоморфна группе Δ ограничений на N автоморфизмов $\sigma \in \Delta'$. Но поле инвариантов группы Δ совпадает с $F \cap N$; описание группы Δ' при помощи группы Δ (теорема 1) немедленно показывает (если рассмотреть базис поля E над $E \cap N$, являющийся одновременно базисом поля $E(N)$ над N), что для инвариантности элемента из $E(N)$ при отображениях из Δ' необходимо и достаточно, чтобы этот элемент принадлежал полю $E(F \cap N)$; из этого следует, что $F = E(F \cap N)$ (определение 1).

Это следствие не обобщается на случай, когда E и N — два расширения поля K, линейно разделенные над K, но такие, что N не является расширением Галуа над K (упражнение 7).

Следствие 2. *Пусть E_1 и E_2 — два таких расширения Галуа поля K, что $E_1 \cap E_2 = K$. Тогда поля E_1 и E_2 линейно разделены над K, причем поле $K(E_1 \cup E_2)$ является расширением Галуа*

поля K, группа Галуа которого изоморфна произведению $\Gamma_1 \times \Gamma_2$ групп Галуа полей E_1 и E_2 над K.

Мы уже видели (предложение 5), что поле $K(E_1 \bigcup E_2)$ является расширением Галуа поля K. Для каждого K-автоморфизма σ_1 (соответственно σ_2) поля E_1 (соответственно E_2) пусть $\bar{\sigma}_1$ (соответственно $\bar{\sigma}_2$) — единственное продолжение σ_1 (соответственно σ_2) до E_2-автоморфизма (соответственно E_1-автоморфизма) поля $K(E_1 \bigcup E_2)$ (теорема 1). Если σ — K-автоморфизм поля $K(E_1 \bigcup E_2)$, то его ограничение на E_1 является K-автоморфизмом σ_1 поля E_1; следовательно, $\bar{\sigma}_1^{-1} \circ \sigma$ есть E_1-автоморфизм $\bar{\sigma}_2$ поля $K(E_1 \bigcup E_2)$. Это показывает, что $\sigma = \bar{\sigma}_1 \circ \bar{\sigma}_2$ и при данном σ, σ_1 и σ_2 определяются однозначно, так как они являются ограничениями автоморфизма σ на поля E_1 и E_2 соответственно. Иными словами, отображение $(\sigma_1, \sigma_2) \to \bar{\sigma}_1 \circ \bar{\sigma}_2$ является взаимно однозначным отображением группы $\Gamma_1 \times \Gamma_2$ на группу Галуа Γ поля $K(E_1 \bigcup E_2)$ над K; это отображение является представлением, так как автоморфизм $(\bar{\sigma}_1 \circ \bar{\sigma}_2) \circ (\bar{\tau}_1 \circ \bar{\tau}_2)$ совпадает с $\sigma_1\tau_1$ на E_1 и с $\sigma_2\tau_2$ на E_2, и поэтому равен $(\overline{\sigma_1\tau_1}) \circ (\overline{\sigma_2\tau_2})$.

5. Теория Галуа

Теорема 2. *Пусть L — поле, Δ — группа автоморфизмов поля L, K — поле инвариантов группы Δ. Для того чтобы L было расширением конечной степени поля K, необходимо и достаточно, чтобы группа Δ была конечной. Поле L тогда будет расширением Галуа поля K, а Δ — группой Галуа поля L над K, и степень поля L над полем K равна порядку группы Δ.*

В самом деле, в силу теоремы Дедекинда (§ 7, теорема 3) элементы группы Δ линейно независимы над L. Поэтому первое утверждение теоремы является немедленным следствием теоремы Артина (§ 7, теорема 1), в которой, кроме того, доказывается, что если порядок группы Δ равен h, то $[L : K] = n$. Следовательно, элементы группы Δ являются единственными K-автоморфизмами поля L (§ 7, предложение 8), откуда следует (определение 1), что L — расширение Галуа поля K, и что Δ — группа Галуа поля L.

Следующая теорема сводит изучение *подрасширений конечного* расширения Галуа к изучению *подгрупп* его группы Галуа.

Теорема 3 (фундаментальная теорема о расширениях Галуа). *Пусть N — расширение Галуа конечной степени поля K, Γ — его группа Галуа; пусть $\mathscr{K}$ — множество полей, лежащих между K и N, и $\mathscr{Y}$ — множество подгрупп группы Γ. Для каждой подгруппы $\Delta \in \mathscr{Y}$ обозначим через $k(\Delta)$ поле инвариантов группы Δ, а для каждого подполя $E \in \mathscr{K}$ через $g(E)$ — группу Галуа поля N над полем E. Соответствие $E \longrightarrow g(E)$ является взаимно однозначным отображением множества $\mathscr{K}$ на множество $\mathscr{Y}$, причем обратным к нему является отображение $\Delta \longrightarrow k(\Delta)$. Для каждого $E \in \mathscr{K}$ порядок группы $g(E)$ равен $[N:E]$, а индекс $(\Gamma : g(E))$ равен $[E:K]$.*

Первое утверждение является непосредственным следствием предложения 2 и теоремы 2, а второе следует из формулы

$$[N:K] = [N:E]\,[E:K].$$

Следствие 1. *Отображение $E \longrightarrow g(E)$ является убывающим отображением множества $\mathscr{K}$ на $\mathscr{Y}$ (упорядоченность по включению). Пусть (E_i) — семейство полей, принадлежащих множеству $\mathscr{K}$, E — их пересечение, F — подполе $K\left(\bigcup_i E_i\right)$. Тогда $g(E)$ — подгруппа в группе Γ, порожденная объединением подгрупп $g(E_i)$, а $g(F)$ совпадает с пересечением подгрупп $g(F_i)$.*

Следствие 2. *Пусть Δ — нормальный делитель группы Γ; тогда поле инвариантов $k(\Delta)$ группы Δ является расширением Галуа поля K.*

Этот результат сразу следует из предложения 4.

Следствие 3. *Для того чтобы промежуточные поля E_1 и E_2 были линейно разделены над K, необходимо и достаточно, чтобы выполнялось равенство*

$$(\Gamma : (g(E_1) \cap g(E_2))) = (\Gamma : g(E_1))\,(\Gamma : g(E_2)).$$

Действительно, если положить $E = K(E_1 \cup E_2)$, то это равенство эквивалентно следующему:

$$[E:K] = [E_1:K]\,[E_2:K],$$

являющемуся критерием линейной разделенности (§ 2, предложение 4).

Следствие 2 из теоремы 1, кроме того, допускает для расширений Галуа конечной степени следующее обращение:

Предложение 7. *Пусть N — конечное расширение Галуа поля K. Если группа Галуа Γ поля N является прямым произведением двух своих подгрупп Γ_1 и Γ_2, то поля инвариантов E_1 и E_2 групп Γ_2 и Γ_1 соответственно являются расширениями Галуа поля K, линейно разделенными над K и $K(E_1 \bigcup E_2) = N$.*

В самом деле, так как подгруппы Γ_1 и Γ_2 являются нормальными делителями в Γ (гл. I, § 6, предложение 6), поля E_2 и E_1 являются расширениями Галуа поля K (следствие 2 теоремы 3), группы Галуа которых соответственно изоморфны группам Γ_2 и Γ_1 (предложение 4); поскольку группа Γ порождается группами Γ_1 и Γ_2, а пересечение $\Gamma_1 \bigcap \Gamma_2$ сводится к единице, то $E_1 \bigcap E_2 = K$ и $N = K(E_1 \bigcup E_2)$ (следствие 1 теоремы 3); следовательно, E_1 и E_2 линейно разделены над K (теорема 1).

Предложение 8. *Если E — конечное алгебраическое сепарабельное расширение конечной степени поля K, то существует лишь конечное число полей, лежащих между K и E.*

В самом деле, нормальное расширение N поля K, порожденное множеством E, является расширением Галуа (предложение 6) конечной степени над K (§ 6, следствие 1 предложения 9); из теоремы 3 следует, что существует лишь конечное число полей, лежащих между K и N, а значит, между K и E.

Обращение этого предложения неверно (упражнение 6).

6. Норма и след в алгебраических сепарабельных расширениях

Определение 2. *Пусть E — алгебраическое сепарабельное расширение поля K, имеющее конечную степень n над K; пусть σ_i $(1 \leqslant i \leqslant n)$ различных K-изоморфизмов поля E в алгебраическое замыкание поля K* (§ 7, предложение 8). *Для каждого элемента $x \in E$ назовем нормой и следом элемента x относительно полей E и K и обозначим соответственно через $\mathrm{N}_{E/K}(x)$ и $\mathrm{Tr}_{E/K}(x)$* (или просто $\mathrm{N}_E(x)$ и $\mathrm{Tr}_E(x)$, или даже через $\mathrm{N}(x)$ и $\mathrm{Tr}(x)$, если не будет возникать недоразумений) *элементы*

$$\mathrm{N}_{E/K}(x) = \sigma_1(x)\,\sigma_2(x)\,\ldots\,\sigma_n(x), \tag{1}$$

$$\mathrm{Tr}_{E/K}(x) = \sigma_1(x) + \sigma_2(x) + \ldots + \sigma_n(x). \tag{2}$$

Из этого определения немедленно следует, что

$$\mathrm{N}_{E/K}(xy) = \mathrm{N}_{E/K}(x)\,\mathrm{N}_{E/K}(y), \tag{3}$$

$$\mathrm{Tr}_{E/K}(x+y) = \mathrm{Tr}_{E/K}(x) + \mathrm{Tr}_{E/K}(y). \tag{4}$$

Элементы $\mathrm{N}_{E/K}(x)$ и $\mathrm{Tr}_{E/K}(y)$ *принадлежат* полю K: в самом деле, нормальное расширение G поля K, порожденное множеством E, является расширением Галуа (предложение 6) и имеет конечную степень над K (§ 6, следствие 1 предложения 9), и для каждого K-автоморфизма τ поля G все K-изоморфизмы $\tau\sigma_i$ поля E различны, поэтому с точностью до порядка совпадают с изоморфизмами σ_i; отсюда $\tau(\mathrm{N}_{E/K}(x)) = \mathrm{N}_{E/K}(x)$ и $\tau(\mathrm{Tr}_{E/K}(x)) = \mathrm{Tr}_{E/K}(x)$, что доказывает наше утверждение (определение 1). Можно, следовательно, говорить, что отображение $x \to \mathrm{Tr}_{E/K}(x)$ является *представлением аддитивной группы* поля E в аддитивную группу поля K, а отображение $x \to \mathrm{N}_{E/K}(x)$, рассматриваемое на *мультипликативной группе* E^* отличных от нуля элементов поля E, является *представлением* этой группы в мультипликативную группу K^* поля K. В частности, $\mathrm{Tr}(-x) = -\mathrm{Tr}(x)$, и если $x \neq 0$, то $\mathrm{N}(x) \neq 0$ и $\mathrm{N}(1/x) = 1/\mathrm{N}(x)$. Для каждого $x \in K$ $\mathrm{Tr}_{E/K}(x) = nx$ и $\mathrm{N}_{E/K}(x) = x^n$.

Замечание. Если E — *расширение Галуа* поля K, то σ_i являются элементами группы Галуа Γ поля E, и можно считать, что отображение $x \to \mathrm{Tr}(x)$ есть умножение на оператор $\sigma_1 + \sigma_2 + \ldots + \sigma_n$ из групповой алгебры A группы Γ над кольцом Z целых рациональных чисел. Более общо, для каждого элемента $\lambda = \sum_{i=1}^{n} h_i\sigma_i$ из этой алгебры и для каждого $x \in E$ положим $\lambda \cdot x = \sum_{i=1}^{n} h_i\sigma_i(x)$; непосредственно видно, что этот внешний закон композиции (вместе со сложением в E) определяет на E структуру *левого A-модуля*.

В том же случае, когда рассматриваются *нормы* элементов из E, предпочтительнее записывать x^σ вместо $\sigma^{-1}(x)$ для каждого $\sigma \in \Gamma$. Положим для каждого элемента $\lambda = \sum_{i=1}^{n} h_i\sigma_i$ из A и каждого $x \in E^*$

$$x^\lambda = \prod_{i=1}^{n} (x^{\sigma_i})^{h_i} = \prod_{i=1}^{n} (x^{h_i})^{\sigma_i}.$$

Следовательно, можно писать $\mathrm{N}(x) = x^{\sigma_1+\sigma_2+\ldots+\sigma_n}$. Легко убедиться, что $(xy)^\lambda = x^\lambda y^\lambda$, $x^{\lambda+\mu} = x^\lambda x^\mu$ и $(x^\lambda)^\mu = x^{\lambda\mu}$; другими словами, закон

умножения *мультипликативной* (абелевой) группы E^* и внешний закон $(\lambda, x) \to x^\lambda$ определяют на E^* структуру *правого* A-модуля.

Предложение 9. *Пусть E — сепарабельное расширение конечной степени n поля K, F — сепарабельное расширение поля E конечной степени m. Для каждого $x \in F$ справедливы равенства*

$$\mathrm{N}_{F/K}(x) = \mathrm{N}_{E/K}(\mathrm{N}_{F/E}(x)), \tag{5}$$

$$\mathrm{Tr}_{F/K}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{F/E}(x)). \tag{6}$$

Действительно, пусть G — расширение Галуа поля K, порожденное множеством F; K-изоморфизмы произвольного подрасширения L расширения G в алгебраическое замыкание поля K отображают L в G и могут быть продолжены до K-автоморфизмов поля G (§ 6, предложение 7). Пусть σ_i $(1 \leqslant i \leqslant n)$ — все K-изоморфизмы поля E в G; предположим, что каждый из них продолжен до некоторого K-автоморфизма поля G, который мы обозначим через $\bar{\sigma}_i$. Пусть, с другой стороны, τ_j $(1 \leqslant j \leqslant m)$ — все E-изоморфизмы поля F в G. Если φ — произвольный K-изоморфизм поля F в G, то его ограничение на E является K-изоморфизмом поля E и, следовательно, совпадает с одним из σ_i. Отображение $\bar{\sigma}_i^{-1} \circ \varphi$ является тогда E-изоморфизмом поля F и, значит, совпадает с некоторым τ_j; другими словами, $\varphi = \bar{\sigma}_i \circ \tau_j$, и ясно, что каждый K-изоморфизм поля F единственным образом записывается в таком виде; следовательно, для каждого $x \in F$

$$\mathrm{Tr}_{F/K}(x) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} \bar{\sigma}_i(\tau_j(x)) \Big) =$$

$$= \sum_{i=1}^{n} \bar{\sigma}_i \Big(\sum_{j=1}^{m} \tau_j(x) \Big) = \sum_{i=1}^{n} \sigma_i(\mathrm{Tr}_{F/E}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{F/E}(x)),$$

поскольку элемент $\mathrm{Tr}_{F/E}(x)$ принадлежит полю E. Аналогично доказывается формула (5).

Следствие 1. *Для каждого элемента $x \in E$ справедливы равенства*

$$\mathrm{N}_{F/K}(x) = (\mathrm{N}_{E/K}(x))^m, \quad \mathrm{Tr}_{F/K}(x) = m \cdot \mathrm{Tr}_{E/K}(x).$$

Следствие 2. *Пусть E — сепарабельное расширение конечной степени n поля K. Пусть еще x — элемент поля E степени m над K, и $f(Z) = Z^m + \sum_{k=1}^{m} a_k Z^{m-k}$ — его минимальный многочлен*

над K. Тогда

$$\mathrm{N}_{E/K}(x) = ((-1)^m a_m)^{\frac{n}{m}}, \tag{7}$$

$$\mathrm{Tr}_{E/K}(x) = -\frac{n}{m} a_1. \tag{8}$$

В самом деле, применим следствие 1 к расширениям $K(x)$ и E и к элементу $x \in K(x)$; пусть x_i $(1 \leqslant i \leqslant m)$ — все сопряженные с элементом x над K, тогда

$$\mathrm{Tr}_{K(x)/K}(x) = \sum_{i=1}^{m} x_i = -a_1 \text{ и } \mathrm{N}_{K(x)/K}(x) = \prod_{i=1}^{m} x_i = (-1)^m a_m,$$

поскольку $f(Z) = \prod_{i=1}^{m} (Z - x_i)$, отсюда следуют формулы (7) и (8).

Предложение 10. *Для всякого сепарабельного расширения E конечной степени поля K существует такой элемент $x \in E$, что* $\mathrm{Tr}_{E/K}(x) \neq 0$.

В самом деле, в противном случае между различными K-изоморфизмами σ_i $(1 \leqslant i \leqslant n)$ поля E существовало бы линейное соотношение $\sum_{i=1}^{n} \sigma_i = 0$, что противоречит теореме Дедекинда (§ 7, теорема 3).

Предложение 11. *Пусть E — сепарабельное расширение конечной степени поля K; для каждого дифференцирования D поля E такого, что $D(E) \subset E$ и для всех $x \in E$ имеем* $\mathrm{Tr}_{E/K}(Dx) = D(\mathrm{Tr}_{E/K}(x))$.

В самом деле, пусть N — расширение Галуа поля K, порожденное множеством E. Дифференцирование D однозначно продолжается на N и $D(N) \subset N$ (§ 9, предложение 5 и следствие 1 предложения 5). Пусть σ_i $(1 \leqslant i \leqslant n)$ — различные K-изоморфизмы поля E в N, продолженные до K-автоморфизмов поля N. Нетрудно проверить, что n отображений $x \to \sigma_i D \sigma_i^{-1}(x)$, определенные в N, являются дифференцированиями, совпадающими с D на поле K. В силу предложения 5, § 9, $\sigma_i D \sigma_i^{-1} = D$, откуда $\sigma_i D(x) = D\sigma_i(x)$ для каждого $x \in E$ $(1 \leqslant i \leqslant n)$. Сложив почленно эти n равенств, получим требуемое утверждение.

Предложение 12. *Пусть E — сепарабельное расширение степени n поля K, $(a_i)_{1 \leqslant i \leqslant n}$ — некоторый базис поля E над K,*

σ_i $(1 \leqslant i \leqslant n)$ — *n различных K-изоморфизмов поля E в алгебраическое замыкание поля K. Тогда*

$$\det(\mathrm{Tr}(a_i a_j)) = (\det(\sigma_i(a_j)))^2. \tag{9}$$

В самом деле, пусть A — матрица $(\sigma_i(a_j))$. Положим ${}^tA \cdot A = (b_{ij})$; тогда $b_{ij} = \sum_{k=1}^{n} \sigma_k(a_i)\,\sigma_k(a_j) = \sum_{k=1}^{n} \sigma_k(a_i a_j) = \mathrm{Tr}(a_i a_j)$. Тем самым все доказано.

Определитель $\det(\mathrm{Tr}(a_i a_j))$ называется *дискриминантом* базиса (a_i) поля E. Он является *ненулевым* элементом поля K (§ 7, замечание, следующее за определением 1).

В главе VIII мы снова вернемся к понятиям следа и нормы как к частным случаям более общих понятий, приложимых к любой *алгебре* конечного ранга над коммутативным кольцом K и, в частности, к *несепарабельным* расширениям поля K; мы увидим также, каким образом эти понятия содержат в себе как частный случай понятия следа и определителя квадратной матрицы (гл. III, §§ 4 и 6).

7. Алгебраическая независимость автоморфизмов

Теорема 4. *Пусть K — бесконечное поле, N — расширение Галуа конечной степени поля K, и пусть σ_i $(1 \leqslant i \leqslant n)$ — все K-автоморфизмы поля N. Пусть Ω — некоторое расширение поля N; если многочлен f, принадлежащий кольцу $\Omega[X_1, X_2, \ldots, X_n]$, удовлетворяет условиям $f(\sigma_1(x), \ldots, \sigma_n(x)) = 0$ для каждого $x \in N$, то $f = 0$.*

Пусть $(a_j)_{1 \leqslant j \leqslant n}$ — базис поля N над K. Каждый элемент $x \in N$ однозначно записывается в виде $x = \sum_{j=1}^{n} y_j a_j$, где $y_j \in K$, следовательно, $\sigma_i(x) = \sum_{j=1}^{n} y_j \sigma_i(a_j)$ $(1 \leqslant i \leqslant n)$. Обозначим через $g(Y_1, Y_2, \ldots, Y_n)$ многочлен

$$f\Big(\sum_{j=1}^{n} \sigma_1(a_j)\,Y_j, \ \ldots, \ \sum_{j=1}^{n} \sigma_n(a_j)\,Y_j\Big)$$

кольца $\Omega[Y_1, \ldots, Y_n]$. По предположению, $g(y_1, \ldots, y_n) = 0$ для всех векторов $(y_j) \in K^n$; следовательно, $g = 0$, так как поле K

бесконечно (гл. IV, § 2, предложение 8). Но матрица $(\sigma_i(a_j))$ обратима (§ 7, замечание, следующее за определением 1), и если (b_{ij}) — обратная для нее матрица, то

$$f(X_1, X_2, \ldots, X_n) = g\Big(\sum_{j=1}^{n} b_{1j}X_j, \ldots, \sum_{j=1}^{n} b_{nj}X_j\Big),$$

следовательно, также $f = 0$.

Теорема неверна, когда поле K *конечно*. В качестве примера возьмем $N = K = Z/(p)$ (p простое); тогда $x^p - x = 0$ для каждого $x \in K$, так как изоморфизм $x \to x^p$ является тождественным автоморфизмом поля K, а многочлен $X^p - X \in K[X]$ не равен нулю.

8. *Нормальный базис расширения Галуа*

Определение 3. *Нормальным базисом расширения Галуа N конечной степени над полем K называется базис, в котором любые два элемента сопряжены.*

Другими словами, если $[N : K] = n$ и если σ_i $(1 \leqslant i \leqslant n)$ — K-автоморфизмы поля N, нормальный базис составляют все сопряженные элементы $\sigma_i(x)$ $(1 \leqslant i \leqslant n)$ элемента $x \in N$. Для того чтобы сопряженные с x элементы составляли нормальный базис, необходимо и достаточно, чтобы $\sigma_i(x)$ были линейно независимы над K. Это условие можно перефразировать так:

Предложение 13. *Для того чтобы сопряженные с $x \in N$ элементы $\sigma_i(x)$ составляли нормальный базис поля N над K, необходимо и достаточно, чтобы* $\det(\sigma_i(\sigma_j(x))) \neq 0$.

Условие достаточно. Действительно, если оно выполнено, то из соотношения $\sum_{j=1}^{n} \lambda_j \sigma_j(x) = 0$, где $\lambda_j \in K$, следует для $1 \leqslant i \leqslant n$, что $\sum_{j=1}^{n} \lambda_j \sigma_i(\sigma_j(x)) = 0$, поскольку $\sigma_i(\lambda_j) = \lambda_j$, откуда $\lambda_j = 0$ для $1 \leqslant j \leqslant n$.

Условие необходимо. Предположим, действительно, что $\det(\sigma_i(\sigma_j(x))) = 0$. Тогда существуют n элементов, не все равные нулю, $\mu_j \in N$ такие, что

$$\sum_{j=1}^{n} \mu_j \sigma_i(\sigma_j(x)) = 0 \quad \text{для} \quad 1 \leqslant i \leqslant n. \tag{10}$$

Так как существует элемент $\alpha \in N$ такой, что $\mathrm{Tr}_{N/K}(\alpha) \neq 0$ (предложение 10), можно считать, что существует по крайней мере один индекс j такой, что $\mathrm{Tr}_{N/K}(\mu_j) \neq 0$ (умножая в случае необходимости уравнения (10) на $\alpha\mu_j^{-1}$ для такого индекса j, что $\mu_j \neq 0$). Иначе уравнения (10) можно записать

$$\sum_{j=1}^{n} \sigma_i^{-1}(\mu_j)\,\sigma_j(x) = 0 \quad (1 \leqslant i \leqslant n), \tag{11}$$

откуда, сложив эти n уравнений (11), получим

$$\sum_{j=1}^{n} \mathrm{Tr}(\mu_j)\,\sigma_j(x) = 0.$$

Так как элементы $\mathrm{Tr}(\mu_j)$ принадлежат K и поскольку по крайней мере один из них не равен нулю, то $\sigma_i(x)$ линейно зависимы над полем K, чем доказательство завершается.

ТЕОРЕМА 5. *Если K — бесконечное поле, то каждое расширение Галуа конечной степени обладает нормальным базисом над полем K.*

Согласно прежним обозначениям положим $\sigma_i\sigma_j = \sigma_{p(i,\,j)}$, где $p(i,\,j)$ — одно из целых чисел $1, 2, \ldots, n$. Рассмотрим многочлен

$$f(X_1, X_2, \ldots, X_n) = \det(X_{p(i,\,j)}),$$

принадлежащий кольцу $K[X_1, X_2, \ldots, X_n]$, и покажем, что $f \neq 0$. В самом деле, ясно, что из соотношения $p(i,\,j) = p(h,\,j)$ следует, что $h = i$, и аналогично из $p(i,\,j) = p(i,\,k)$ следует, что $j = k$. Следовательно, значение $f(1, 0, \ldots, 0)$ является определителем матрицы, имеющей единственный не равный нулю элемент (равный 1) в каждой строке и каждом столбце, другими словами, матрицы подстановки (гл. II, § 6, n° 5); следовательно, $f(1, 0, \ldots, 0) = \pm 1$, что доказывает наше утверждение. Так как $\det(\sigma_i(\sigma_j(x))) = f(\sigma_1(x), \ldots, \sigma_n(x))$, теорема 4 показывает, что существует такой элемент $x \in N$, что $\sigma_i(\sigma_j(x)) \neq 0$, следовательно (предложение 13), сопряженные с x элементы образуют нормальный базис поля N над K.

Можно показать, что теорема 5 распространяется на случай, когда K *конечное* поле (гл. VII, § 5, n° 7).

9. Нормальные несепарабельные расширения

Предложение 14. *Пусть K — поле характеристической экспоненты p, Ω — алгебраическое замыкание поля K, N — нормальное расширение поля K, содержащееся в Ω, $\widetilde{N}$ — поле инвариантов группы K-автоморфизмов поля N, N_0 — наибольшее сепарабельное расширение поля K, содержащееся в N. Тогда*: а) *$\widetilde{N}$ — наибольшее радикальное расширение, содержащееся в N, другими словами, $\widetilde{N} = N \cap K^{p^{-\infty}}$*; б) *$N_0$ — расширение Галуа поля K, линейно разделенное с $\widetilde{N}$ над K, и каждый K-автоморфизм поля N_0 единственным образом продолжается до K-автоморфизма поля N*; в) $N = K(N_0 \cup \widetilde{N})$ (рис. 4).

$$\begin{array}{ccc} \widetilde{N} & \longrightarrow & N \\ \uparrow & & \uparrow \\ K & \longrightarrow & N_0 \end{array}$$

Рис. 4.

Каждый элемент поля N, радикальный над K, можно перевести в другой элемент некоторым K-автоморфизмом поля Ω, ограничение которого на поле N является K-автоморфизмом поля N; следовательно, $\widetilde{N} = N \cap K^{p^{-\infty}}$.

Если $x \in N$ сепарабелен над K, то все сопряженные с ним над полем K элементы также сепарабельны (§ 7, следствие 1, предложение 9) и, следовательно, принадлежат полю N_0. Это показывает, что N_0 нормально, и поэтому (предложение 1) является расширением Галуа поля K. Поскольку N_0 линейно разделено с полем $K^{p^{-\infty}}$ (§ 8, предложение 3), оно тем более разделено с полем $\widetilde{N}$. С другой стороны, N является радикальным расширением поля N_0 (§ 8, следствие предложения 7), и следовательно (§ 6, предложение 7), каждый K-автоморфизм поля N_0 однозначно продолжается до K-автоморфизма поля N. Но поле N является расширением Галуа поля $\widetilde{N}$ по определению (определение 1) и каждый K-автоморфизм поля N является $\widetilde{N}$-автоморфизмом.

Покажем, наконец, что $N = K(N_0 \cup \widetilde{N})$. Можно ограничиться случаем, когда N имеет *конечную степень над K*. В самом деле,

пусть x — какой-нибудь элемент из N; тогда нормальное расширение M, порожденное множеством $K(x)$, имеет конечную степень над K (§ 6, следствие 1, предложение 9). Пусть M_0 (соответственно $\widetilde{M}$) — наибольшее сепарабельное (соответственно радикальное) расширение поля K, содержащееся в M; если мы докажем, что $x \in K(M_0 \cup \widetilde{M})$, тогда $x \in K(N_0 \cup \widetilde{N})$, поскольку $M_0 \subset N_0$ и $\widetilde{M} \subset \widetilde{N}$.

Мы можем считать поэтому, что степень $[N:K]$ конечна. В силу б) группы Галуа полей N_0 над K и N над $\widetilde{N}$ изоморфны, поэтому $[N_0:K]=[N:\widetilde{N}]$ (теорема 3) и следовательно, $N=K(N_0 \cup \widetilde{N})$ (§ 2, предложение 4).

Упражнения. *1) Пусть Ω — некоторое тело (*не обязательно коммутативное*), $\mathcal{G}$ — группа автоморфизмов тела Ω, L — поле инвариантов группы $\mathcal{G}$. Пусть N — такое подтело в Ω, что $\sigma(N)=N$ для каждого автоморфизма $\sigma \in \mathcal{G}$. Показать, что расширение N сепарабельно (§ 8, упражнение 2) над полем $K=N \cap L$; пусть (a_λ) — семейство элементов из L, линейно независимых (слева) над K; показать, что они также линейно независимы над N, рассматривая первичное соотношение между элементами a_λ с коэффициентами из N; вывести отсюда, что каждое линейно независимое (справа) семейство элементов (b_μ) из N линейно независимо (справа) над L).

2) Пусть N_1 и N_2 — два расширения Галуа поля K, N_0 — их пересечение, N — поле $K(N_1 \cup N_2)$. Обозначим через Γ_1, Γ_2 и Γ группы полей N_1, N_2 и N, соответственно над полем K, а через Δ_1 и Δ_2 — группы полей N_1 и N над полем N_0. Каждому классу $\overline{\sigma}_1$ по модулю Δ_1 в Γ_1 соответствует класс $\overline{\sigma}_2$ по модулю Δ_2 в группе Γ_2, состоящий из автоморфизмов из Γ_2, ограничение которых на поле N_0 совпадает с ограничением на N_0 всех автоморфизмов, принадлежащих классу $\overline{\sigma}_1$. Определенное таким образом соответствие является изоморфизмом φ групп Γ_1/Δ_1 и Γ_2/Δ_2. Показать, что группа Γ изоморфна подгруппе θ произведения групп $\Gamma_1 \times \Gamma_2$, состоящей из таких пар (σ_1, σ_2), что $\overline{\sigma}_1$ и $\overline{\sigma}_2$ являются соответствующими при изоморфизме φ классами в Γ_1 и Γ_2, т. е. $\overline{\sigma}_2=\varphi(\overline{\sigma}_1)$ (используйте теорему 1).

3) Пусть f — многочлен кольца $K[X]$, имеющий лишь простые корни в алгебраическом замыкании поля K. Для того чтобы группа Галуа поля корней многочлена f была транзитивной (когда она рассматривается как группа подстановок корней многочлена f), необходимо и достаточно, чтобы многочлен f был неприводим.

4) Пусть f — неприводимый сепарабельный многочлен из $K[X]$ и Γ — группа Галуа над K поля корней многочлена f, рассматриваемая как транзитивная группа перестановок корней многочлена f.

Показать, что для того, чтобы поле $K(x_i)$, получаемое присоединением к полю K одного из корней многочлена f, содержало подполе $E \supset K$, отличное от K и $K(x_i)$, необходимо и достаточно, чтобы группа Г была импримитивной (гл. I, § 7, n° 7).

5) Пусть f — неприводимый и сепарабельный многочлен из $K(x)$ степени n, α_i $(1 \leqslant i \leqslant n)$ — его корни, $N = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — его поле корней. Пусть F — поле рациональных дробей $N(X_1, \ldots, X_n)$, E — подполе $K(X_1, \ldots, X_n) \subset F$. Поле F является расширением Галуа поля E, группа Галуа которого изоморфна группе Галуа Г поля N над K. Показать, что если $\theta = \alpha_1 X_1 + \alpha_2 X_2 + \ldots + \alpha_n X_n$, то $F = E(\theta)$, и что минимальный над E многочлен элемента θ является некоторым неприводимым множителем g_1 многочлена

$$f(X) = \prod_{\pi} (X - \alpha_1 X_{\pi(1)} - \alpha_2 X_{\pi(2)} - \ldots - \alpha_n X_{\pi(n)}),$$

где π пробегает симметрическую группу $\mathfrak{S}_n$. Каждая подстановка π определяет K-автоморфизм поля E, который мы также обозначим через π, такой, что $\pi(X_i) = X_{\pi(i)}$ $(1 \leqslant i \leqslant n)$. Показать, что группа Г изоморфна подгруппе группы $\mathfrak{S}_n$, образованной такими подстановками π, что $\pi(g_1) = g_1$. Далее, пусть $f = g_1 g_2 \ldots g_r$ — разложение f на неприводимые множители в кольце $E[X]$; показать, что для каждого индекса k существует такая подстановка $\pi_k \in \mathfrak{S}$, что $\pi_k(g_1) = g_k$.

*6) Пусть K — несовершенное поле характеристики $p > 0$, и пусть E — алгебраическое расширение конечной степени поля K.

а) Показать, что если степень несовершенности поля E над K (§ 8, упражнение 1) больше 1, то существует бесконечно много различных полей F, лежащих между E и K (свести к случаю, когда $K(E^p) = K$; пусть a и b — два p-независимых над K элементов поля E, тогда все поля $K(a + \lambda b)$ различны, когда λ пробегает K).

б) Обратно, показать, что если степень несовершенности поля E над K равна 1, то существует лишь конечное число полей, лежащих между E и K (использовать упражнение 4, § 8 и предложения 8, 10).

7) Пусть N — расширение Галуа поля K, группа Галуа Г которого изоморфна симметрической группе $\mathfrak{S}_n$, с которой она и отождествляется (см. Приложение 1, предложение 2). Пусть n — целое непростое число. Обозначим через Δ_1 подгруппу группы $\mathfrak{S}_n$ порядка $(n-1)!$, оставляющую на месте число 1, а через Δ_2 — циклическую подгруппу порядка n в $\mathfrak{S}_n$, порожденную циклом (1, 2, 3, ...) (гл. I, § 7, упражнение 6).

Пусть E_1 и E_2 — поля инвариантов подгрупп Δ_1 и Δ_2 группы Г. Показать, что E_1 и E_2 линейно разделены над K и что не существует поля, лежащего между E_1 и K, отличного от этих двух полей, хотя существуют поля, лежащие между N и F_2, отличные от N и E_2.

8) Пусть E — сепарабельное расширение поля K, имеющее над K конечную степень, N — расширение Галуа поля K, порожденное множеством E, α — элемент из N, все сопряженные элемеяты которого составляют нормальный базис поля N над K. Пусть $\beta = \mathrm{Tr}_{N/E}(\alpha)$; показать, что $E = K(\beta)$.

9) Пусть E и F — два расширения Галуа полн K, имеющие над K конечную степень и такие, что $E \cap F = K$; пусть α (соответственно β) — элемент из E (соответственно F), все сопряженные над K элементы которого образуют нормальный базис поля E (соответственно F) над K. Показать, что в поле $K(E \cup F)$ все сопряженные с $\alpha\beta$ над K элементы образуют над K нормальный базис.

*10) Пусть K — поле характеристики $p \neq 2$ и $E = K(x)$ — поле рациональных дробей от одного переменного над K. Пусть σ и τ — инволютивные K-автоморфизмы поля E, которые каждой рациональной дроби $f(X)$ ставят в соответствие $f(-X)$ и $f(1-X)$ соответственно.

а) Показать, что полями инвариантов этих автоморфизмов σ и τ являются соответственно $K(X^2)$ и $K(X^2 - X)$ (см. теорему 3 и § 5, упражнение 5);

б) если $p = 0$, то группа, порожденнан σ и τ, бесконечна. Отсюда следует, что $K(X^2) \cap K(X^2 - X) = K$. Если же $p > 2$, то $K(X^2) \cap \cap K(X^2 - X) = K(X^2(X^{p-1} - 1)^2)$ (тем же методом, что и в случае а)).

11) Пусть E — алгебраическое расширение поля K характеристики $p > 0$, E_0 — наибольшее сепарабельное расширение поля K, содержащееся в E, $\widetilde{E} = E \cap K^{p^{-\infty}}$ — наибольшее радикальное расширение поля K, содержащеесн в E. Если N — нормальное расширение поля K, порожденное множеством E, то наибольшее сепарабельное расширение полн K, содержащееся в N, совпадает с расширением Галуа N_0 поля K, порожденное полем E_0. Для того чтобы поле $\widetilde{N} = N \cap K^{p^{-\infty}}$ совпадало с $\widetilde{E}$, необходимо и достаточно, чтобы E было сепарабельно над $\widetilde{E}$.

12) Пусть E — некоторое алгебраическое расширение поля K, Γ — группа K-автоморфизмов поля E, S — поле инвариантов группы Γ.

а) Чтобы E было нормальным над K, необходимо и достаточно, чтобы S было радикально над K;

б) пусть S_0 — наибольшее сепарабельное расширение полн K, содержащееся в S. Показать, что S_0 — наименьшее среди полей F, лежащих между K и E, таких, что E является нормальным расширением поля F;

в) пусть E_0 — наибольшее сепарабельное расширение поля K, содержащееся в E. Показать, что $E = S(E_0)$ (заметить, что никакой K-автоморфизм поля E, отличный от тождественного, не оставляет инвариантными все элементы из $S(E_0)$).

§ 11. Корни из единицы. Конечные поля. Циклические расширения

1. Корни из единицы

Определение 1. *Элемент x поля K называется корнем из единицы, если существует целое положительное число n, для которого $x^n=1$. Всякий элемент x, для которого $x^n=1$, называется корнем n-й степени из единицы.*

То же можно выразить, сказав, что корни из единицы — это элементы *конечного порядка* мультипликативной группы K^* ненулевых элементов поля K (гл. I, § 6, n° 7). Корни из единицы образуют подгруппу $S(K)$ группы K^*, а корни n-й степени из единицы — подгруппу группы $S(K)$. Пусть задан некоторый корень n-й степени x из единицы, тогда множество целых рациональных чисел m, для которых $x^m=1$, является прообразом единичного элемента 1 при представлении $h\to x^h$ аддитивной группы Z в мультипликативную группу K^*. Следовательно, это множество является подгруппой nZ группы Z, где n — наименьшее из положительных целых чисел m, для которых $x^m=1$, то есть *порядок* (гл. I, § 6, n° 7) элемента x в группе K^*.

Пусть p — характеристика поля K. Если элемент $x\in K$ является корнем из единицы, то его порядок *не делится* на p. В самом деле, если $p\neq 0$, то из соотношения $x^{mp}=1$, которое можно записать в виде $(x^m-1)^p=0$ (§ 1, предложение 1), вытекает, что $x^m=1$, причем $m<mp$.

Всякий корень n-й степени из единицы в поле K алгебраичен над *простым подполем p поля K*, так как он является корнем многочлена X^n-1. В этом параграфе все встречающиеся поля мы будем рассматривать как подполя одного и того же алгебраически замкнутого расширения Ω поля P. Если n — целое положительное число, которое не делится на характеристику p поля P, то любой корень многочлена X^n-1 *прост*. Действительно, производная nX^{n-1} этого многочлена обращается в нуль только при нулевом значении x, которое не является корнем многочлена X^n-1. Таким образом, существует n *корней n-й степени из единицы* в поле Ω. Любой корень из единицы, будучи алгебраичным над полем P, к тому же *сепарабелен* над P, потому что P — совершенное поле.

Отметим, что поле K может не содержать никакого корня n-й степени из единицы, кроме самой единицы. Например, это имеет место в случае простого поля Q при любом нечетном целом n.

Теорема 1. *Пусть P — простое поле характеристики p, n — целое положительное число, которое не делится на p. Группа корней n-й степени из единицы* (во всяком алгебраически замкнутом расширении Ω поля P) *является циклической группой n-го порядка.*

Мы используем несколько предварительных лемм.

Напомним, что наибольший общий делитель (н. о. д.) d двух положительных целых рациональных чисел m и n выделяется из множества всех положительных общих делений чисел m и n тем, что существуют целые рациональные числа h, k, для которых $d = hm + kn$ (гл. I, § 8, n° 6). Из этого следует, что для любого положительного целого числа r н. о. д. чисел rm и rn равен rd. Числа m и n называются *взаимно простыми* (а каждое из чисел — *простым относительно другого*), если их н. о. д. равен единице.

Лемма 1. *Для того чтобы смежный класс по модулю n положительного целого числа x порождал циклическую группу $Z/(n)$, необходимо и достаточно, чтобы числа x, n были взаимно просты.*

Действительно, необходимо и достаточно, чтобы класс элемента x имел порядок n в группе $Z/(n)$, то есть чтобы из соотношения $xy \equiv 0 \pmod{n}$ (где y — целое) вытекало сравнение $y \equiv 0 \pmod{n}$. Но это означает, что в *кольце* $Z/(n)$ класс u элемента x *не является делителем нуль*. В этом случае отображение $v \to uv$ кольца $Z/(n)$ в себя взаимно однозначно. Ввиду конечности кольца $Z/(n)$ оно является отображением кольца $Z(n)$ *на* себя. Таким образом, элемент u *обратим* в кольце $Z/(n)$. Обратное утверждение получается немедленно. Но это и означает, что существует два целых числа h, k, для которых $hx = 1 + kn$. Следовательно, числа x и n взаимно просты.

Количество целых положительных чисел x, *взаимно простых* с n и не превосходящих n, обозначается символом $\varphi(n)$ и называется *функцией Эйлера* от n. Таким образом, ее значения являются *числом образующих в циклической группе порядка n* (гл. I, § 6, предложение 8), а также *числом обратимых элементов в кольце* $Z/(n)$.

Лемма 2. *Для любого целого положительного числа n справедливо равенство*

$$\sum_{d/n} \varphi(d) = n, \tag{1}$$

в котором целое число d пробегает множество положительных делителей n).*

Действительно, найдем количество целых x, $1 \leqslant x \leqslant n$, для которых н. о. д. x и n равен заданному делителю δ числа n. В этом случае $\delta = hx + kn$ для некоторых целых рациональных чисел h, k, откуда следует, что $1 = h\frac{x}{\delta} + k\frac{n}{\delta}$. Это доказывает взаимную простоту чисел x/δ и $n/\delta = d$; обратное получается немедленно. Ввиду того, что $\frac{x}{\delta} \leqslant d$, искомое количество равно $\varphi(d)$. Когда δ пробегает множество положительных делителей числа n, то же множество пробегает и $d = n/\delta$. Из этого вытекает формула (1).

Лемма 3. *Пусть G — конечная группа порядка n. Если для любого целого положительного делителя d числа n число элементов группы G, порядок которых делит d, не больше чем d, то группа G циклическая.*

В самом деле, пусть d — положительный делитель n. Если в группе G существует элемент x порядка d, то порядки всех d различных элементов x^r $(0 \leqslant r \leqslant d-1)$ делят d. Таким образом, это *единственные* элементы группы G, порядки которых делят d. Следовательно, число элементов группы G порядка d в этом случае равно числу образующих циклической группы, порожденной элементом x, т. е. $\varphi(d)$ (лемма 1). Порядок любого элемента группы G делит n (гл. I, § 6, n° 7). Из соотношения (1) вытекает, что для *любого* положительного делителя d числа n *существует* $\varphi(d)$ элементов группы G порядка d. В частности, существует $\varphi(n)$ элементов группы G порядка n, каждый из которых, следовательно, порождает группу G. ◻

Доказав эти леммы, покажем, что лемму 3 можно применить к группе корней n-й степени из единицы в поле Ω. Действительно, при любом положительном делителе d числа n для корня из единицы x, порядок которого делит d, справедливо соотноше-

*) Соотношение d/n между положительными целыми числами означает, что d делит n (см. гл. V, § 1, n° 5).

ние $x^d = 1$ и обратно. Таким образом, имеется точно d корней из единицы, порядок которых делит d, что доказывает требуемое.

Корень n-й степени из единицы называется *примитивным*, если его порядок равен n, то есть если он *порождает* группу корней n-й степени из единицы. При доказательстве теоремы 1 мы показали, что:

Следствие. *Для любого целого положительного числа n, которое не делится на p, число примитивных корней n-й степени из единицы равно $\varphi(n)$.*

Предложение 1. *Пусть Ω — алгебраически замкнутое поле характеристики p. Группа $S(\Omega)$ корней из единицы в Ω изоморфна группе S_p/Z, где S_p — подгруппа аддитивной группы Q, образованная дробями r/s, у которых s не делится на p.*

Заметим сначала, что из соотношения $st \equiv 0 \pmod p$ следует, что либо $s \equiv 0 \pmod p$, либо $t \equiv 0 \pmod p$, поскольку кольцо $Z/(p)$ — кольцо целостности. Таким образом, множество S_p действительно является подгруппой группы Q. Пусть (ν_n) — строго возрастающая последовательность всех целых чисел, которые не делятся на p. Положим $\lambda_n = \nu_1\nu_2 \dots \nu_n$. Обозначим через H_n группу корней λ_n-й степени из единицы. При этом $H_{n+1} \supset H_n$ и $S(\Omega) = \bigcup\limits_n H_n$. Поскольку группа H_n — циклическая порядка λ_n, то существует последовательность (α_n) корней из единицы, где α_n — примитивный корень λ_n-й степени из единицы и $\alpha_n = \alpha_{n+1}^{\nu_n+1}$. Далее, любой элемент $x \in S_p$ можно записать в виде r/λ_n (и притом бесконечным множеством способов). В силу определения α_n элемент α_n^r не зависит от записи r/λ_n элемента x. Мы обозначим элемент α_n^r в группе $S(\Omega)$ символом $f(x)$. Очевидно, что f — представление S_p в $S(\Omega)$, отображающее S_p на $S(\Omega) = \bigcup\limits_n H_n$. С другой стороны, соотношение $f(r/\lambda_n) = 1$ означает, что $\alpha_n^r = 1$, то есть что r/λ_n — целое число. Таким образом, группа $S(\Omega)$ изоморфна группе S_p/Z.

2. *Поле корней n-й степени из единицы*

Пусть K — поле характеристики p, n — целое число, которое не делится на p. Назовем *полем корней n-й степени из единицы* над полем K и обозначим символом $R_n(K)$ поле корней много-

члена X^n-1 над полем K (§ 4, n° 2). Так как этот многочлен сепарабелен, то поле $R_n(K)$ является расширением *Галуа* конечной степени поля K (см. § 10, следствие предложения 6). Если ζ — некоторый примитивный корень n-й степени из единицы, то любой корень n-й степени из единицы является степенью ζ.

Таким образом, $R_n(K)=K(\zeta)$.

Пусть Γ — группа Галуа поля $R_n(K)$ относительно поля K. Для любого элемента $\sigma\in\Gamma$ элемент $\sigma(\zeta)$ должен быть примитивным корнем n-й степени из единицы. Следовательно, $\sigma(\zeta)=\zeta^r$, где r — целое число, смежный класс которого по модулю n является вполне определенным элементом мультипликативной группы обратимых элементов в кольце $Z/(n)$ (следствие из теоремы 1). Этот элемент мы обозначим символом $\chi(\sigma)$. Пусть τ — второй автоморфизм из группы Γ, причем $\tau(\zeta)=\zeta^s$; тогда $\sigma(\tau(\zeta))=\sigma(\zeta^s)=(\sigma(\zeta))^s=\zeta^{rs}$. Отсюда следует, что $\chi(\sigma\tau)=\chi(\sigma)\chi(\tau)$. Другими словами, отображение $\sigma\to\chi(\sigma)$ является *представлением* группы Γ на подгруппу мультипликативной группы обратимых элементов в кольце $Z/(n)$. Более того, представление $\sigma\to\chi(\sigma)$ является *изоморфизмом*, поскольку два K-автоморфизма поля $R_n(K)$ совпадают, если они имеют одинаковые значения на элементе ζ (§ 6, n° 2). В итоге:

Предложение 2. *Пусть K — поле характеристики p, n — целое положительное число, которое не делится на p. Поле $R_n(K)$ корней n-й степени из единицы над полем K является абелевым расширением конечной степени поля K, группа Галуа которого изоморфна подгруппе мультипликативной группы обратимых элементов кольца $Z/(n)$.*

Отсюда вытекает, что степень $[R_n(K):K]$ является *делителем* числа $\varphi(n)$.

Отметим, что $R_n(K)=K(R_n(P))$. Таким образом, группа Галуа поля $R_n(K)$ над полем K изоморфна группе Галуа поля $R_n(P)$ над $K\cap R_n(P)$ (§ 10, теорема 1), т. е. подгруппе группы Галуа Γ_0 поля $R_n(P)$ над полем P.

Мы увидим далее, что при $p=0$ группа Галуа Γ_0 поля $R_n(Q)$ над Q изоморфна группе *всех* обратимых элементов кольца $Z/(n)$ и, следовательно, имеет порядок $\varphi(n)$. Но это уже не так, если $p>0$.

Положим $h=\varphi(n)$. Пусть ζ_i $(1\leqslant i\leqslant h)$ — h примитивных корней из единицы. Многочлен $\Phi_n(X)=\prod_{i=1}^{h}(X-\zeta_i)$ принадлежит кольцу $P[X]$, ибо он инвариантен при любом автоморфизме из группы Γ_0. Уравнение $\Phi_n(x)=0$ называется *уравнением деления круга на n равных частей* или *циклотомическим уравнением индекса n*. Многочлен Φ_n называют *циклотомическим многочленом индекса n*. Многочлен Φ_n неприводим в кольце $P[X]$ в том и только в том случае, если группа Γ_0 имеет порядок, равный $\varphi(n)$.

Если число n задано явно, можно явно вычислить многочлен Φ_n с помощью следующего рекуррентного процесса. Если корень n-й степени из единицы имеет порядок d, то d делит n (№ 1) и x является примитивным корнем степени d. Обратно, любой примитивный корень степени d является корнем n-й степени из единицы, если d делит n. Таким образом, имеем

$$X^n-1=\prod_{d/n}\Phi_d(X). \tag{2}$$

Это определяет $\Phi_n(X)$, если известны $\Phi_n(X)$ для всех делителей d (строго меньших n) числа n. Так как $\Phi_1(X)=X-1$, то имеем, таким образом, рекуррентный процесс, определяющий Φ_n. Например, если $h=q$ — простое число, то

$$X^q-1=(X-1)\,\Phi_q(X),$$

откуда

$$\Phi_q(X)=X^{q-1}+X^{q-2}+\ldots+X+1.$$

В качестве другого примера вычислим $\Phi_{12}(X)$. Имеем

$$X^{12}-1=\Phi_{12}\Phi_6\Phi_4\Phi_3\Phi_2\Phi_1$$

и

$$X^6-1=\Phi_6\Phi_3\Phi_2\Phi_1,$$

откуда

$$X^6+1=\Phi_{12}\Phi_4.$$

Но

$$X^4-1=\Phi_4\Phi_2\Phi_1.$$

Так как $\Phi_1(X)=X-1$, а $\Phi_2(X)=X+1$, то $\Phi_4(X)=X^2+1$. Отсюда, окончательно,

$$\Phi_{12}(X)=X^4-X^2+1.$$

Отметим, что многочлен $\Phi_{12}(X)$ приводим над полем характеристики 5, поскольку

$$X^4-X^2+1=(X^2-2X-1)(X^2+2X-1)$$

(см. упражнение 1).

Замечания. 1) Сравнивая степени двух членов в равенстве (2), найдем соотношение (1). Отсюда можно вывести аналогичный рекур-

рентный процесс для вычисления $\varphi(n)$. Позднее мы дадим другие выражения для $\varphi(n)$ и многочлена Φ_n.

2) Метод вычисления Φ_n, указанный выше, дает для Φ_n многочлен с целыми рациональными коэффициентами, которые определены однозначно (как это легко доказать индукцией) и не зависят от характеристики поля P.

3. *Конечные поля*

Мы докажем в главе VIII, § 11, n° 1, что любое конечное тело обязательно *коммутативно* (см. упражнение 14). В этом n° мы изучим структуру конечных тел, предполагая их коммутативными.

Мы уже заметили (§ 1, n° 1), что конечное поле K необходимо имеет характеристику $p > 0$ (которая, следовательно, совпадает с характеристической экспонентой поля K). Оно является расширением своего простого подполя P (изоморфного полю $Z/(p)$), причем, очевидно, конечной степени n над P. Напомним, что любое некоторое пространство E размерности n над полем L изоморфно пространству L^n (гл. II, § 3, следствие 1 к теореме 3). Если поле L состоит из r элементов, то векторное пространство E содержит r^n элементов. Это доказывает, что рассматриваемое поле K имеет $p^n = q$ элементов.

Мультипликативная группа K^* ненулевых элементов поля K является группой порядка $q-1$. Следовательно, для любого элемента x из K^* имеем $x^{q-1} = 1$ (гл. I, § 6, следствие к предложению 8), и тем более $x^q = x$. Это последнее соотношение справедливо и при $x = 0$. Поэтому мы видим, что q элементов ξ_i $(1 \leqslant i \leqslant q)$ поля K являются корнями многочлена $X^q - X$, откуда следует тождество $X^q - X = \prod_{i=1}^{q} (X - \xi_i)$. Таким образом, можно сказать, что поле K совпадает одновременно *с полем корней* и с *множеством корней* многочлена $X^q - X$. Это доказывает изоморфизм двух конечных полей с одним и тем же числом элементов *).

*) В самом деле, пусть p_1 и p_2 — два различных простых числа; тогда $p_1^m \neq p_2^n$ для любых целых положительных чисел m и n. Иначе из равенства $p_2^n = p_1^m$ вытекало бы, что $p_2^n \equiv 0 \pmod{p_1}$. Ввиду того, что $Z/(p_1)$ — поле, в нем отсутствуют делители 0. Отсюда получим, что $p_2 \equiv 0 \pmod{p_1}$, что невозможно (см. гл. VII, § 1, n° 3).

Обратно, пусть $q=p^n$ — любая степень некоторого простого числа p. Рассмотрим в алгебраическом замыкании Ω_p простого поля Z/p корни многочлена X^q-X, или, что то же самое, элементы поля Ω_p, инвариантные при автоморфизме $x\to x^q$ совершенного поля Ω_p (§ 1, предложение 1 и § 7, следствие предложения 5). Эти элементы образуют поле, которое мы обозначим (для удобства) символом F_q. Это поле является расширением конечной степени поля $Z/(p)=F_p$. Так как производная многочлена X^q-X равна -1, то все корни многочлена X^q-X в Ω_p простые (глава IV, § 4, предложение 3). Следовательно, поле F_q содержит $q=p^n$ элементов и является расширением Галуа поля F_p (§ 10, следствие предложения 6) степени n. Мультипликативная группа F_q^* ненулевых элементов поля F_q совпадает с группой корней $(q-1)$-й степени из единицы в поле Ω_p. В итоге:

Теорема 2. а) *Число элементов q конечного поля необходимо является степенью p^n некоторого простого числа p.*

б) *Для любого простого числа p и любого целого числа $n>0$ существует поле F_q, состоящее из $q=p^n$ элементов: поле корней многочлена X^q-X над простым полем $F_p=Z/(p)$. Любой элемент поля F_q является корнем этого многочлена.*

в) *F_q есть поле инвариантов относительно автоморфизма $x\to x^q$ (произвольного) алгебраически замкнутого расширения поля F_q.*

г) *Любое поле из q элементов изоморфно полю F_q.*

д) *Аддитивная группа поля F_q является прямой суммой n циклических групп порядка p. Мультипликативная группа F_q^* является циклической группой порядка $q-1$.*

4. Алгебраические расширения конечной степени конечного поля

Предложение 3. а) *Для любого целого $m>0$ поле F_{q^m} является расширением степени m поля F_q. Для любого образующего ζ циклической группы $F_{q^m}^*$ имеем $F_{q^m}=F_q(\zeta)$.*

б) *В произвольном алгебраически замкнутом расширении Ω поля F_q существует единственное расширение степени m поля F_q, изоморфное полю F_{q^m}.*

Первая часть предложения получается немедленно. С другой стороны, всякое расширение степени m поля F_q, содержащееся

в Ω, состоит из q^m элементов. Следовательно (теорема 2 в)) оно является полем инвариантов автоморфизма $x \to x^{q^m}$ в поле Ω, чем и заканчивается доказательство.

Следствие. *Каждый ненулевой элемент алгебраического замыкания конечного поля является корнем из единицы.*

Действительно, если элемент x алгебраичен над полем F_q, то $F_q(x)$ есть алгебраическое расширение конечной степени поля F_q, следовательно, конечное поле.

Первая часть предложения 3 позволяет сформулировать теорему о примитивных элементах (§ 7, предложение 12) во всей ее общности:

Предложение 4. *Каждое сепарабельное алгебраическое расширение E конечной степени над полем K является простым.*

Предложение 5. *Поле F_{q^m} является абелевым расширением поля F_q. Его группа Галуа над полем F_q является циклической группой порядка m и состоит из автоморфизмов $x \to x^k$ $(0 \leqslant k \leqslant m-1)$.*

Действительно, пусть σ — автоморфизм $x \to x^q$ поля F_{q^m} (§ 7, следствие к предложению 5). Полем инвариантов для автоморфизма σ служит поле F_q (теорема 2). Следовательно, оно является и полем инвариантов для циклической группы Γ, порожденной σ. Из этого вытекает (§ 10, теорема 2), что Γ является группой Галуа поля F_{q^m} над полем F_q и имеет, таким образом, порядок, равный m.

5. Циклические расширения

Определение 2. *Расширение E поля K называется циклическим, если оно является расширением Галуа, а его группа Галуа над полем K циклическая.*

Примеры. 1) Каждое сепарабельное *квадратичное* расширение E поля K циклично над полем K. В самом деле (§ 7, предложение 12), имеем $E = K(\omega)$, где ω — корень некоторого неприводимого многочлена $X^2 + \alpha X + \beta$ из кольца $K[X]$. Второй корень ω' этого многочлена равен $\alpha - \omega$ и, значит, также принадлежит полю E. Поле E является расширением Галуа поля K, его группа Галуа над K имеет порядок, равный двум, и, значит, циклична.

2) Предложение 5 показывает, что поле F_{q^m} является циклическим расширением степени m поля F_q.

3) Пусть K — произвольное поле, σ — автоморфизм конечного порядка n поля K (то есть n — это наименьшее из целых чисел h, для которых σ^h есть тождественный автоморфизм). Поле L инвариантов автоморфизма σ в то же время есть и поле инвариантов циклической группы n-го порядка, порожденной σ. Следовательно (§ 10, теорема 2), поле K является циклическим расширением степени n поля L.

Известно (гл. I, § 6, предложение 8), что каждая циклическая группа n-го порядка изоморфна группе $Z/(nZ)$. Подгруппы группы Z, содержащие nZ, имеют вид dZ, где d пробегает множество делителей числа n. Поэтому подгруппы группы Z/nZ являются факторгруппами вида dZ/nZ (гл. I, § 6, теорема 6). Но если $n = d\delta$, то изоморфиэм $x \longrightarrow dx$ группы Z на dZ отображает подгруппу δZ группы Z на подгруппу nZ группы dZ. Таким образом, группа dZ/nZ изоморфна группе $Z/\delta Z$. С другой стороны, факторгруппа группы Z/nZ по подгруппе dZ/nZ изоморфна группе Z/dZ (гл. I, § 6, теорема 6). Тем самым, мы видим, что каждая *подгруппа* и каждая *факторгруппа* циклической группы опять являются циклической группой. Таким образом (§ 10, теорема 3 и предложение 4), если E — циклическое расширение степени n поля K, то любое поле F, промежуточное между K и E, *циклично* над K, а поле E *циклично* над F. Точнее, имеется взаимно однозначное соответствие между делителями числа n и промежуточными полями между K и E: каждому делителю d числа n соответствует промежуточное циклическое поле F степени n/d над полем K, для которого E — циклическое поле степени d над полем F.

В произвольном циклическом расширении E поля K норма и след элемента поля E обладают следующим фундаментальным свойством:

Теорема 3 (Гильберт). *Пусть E — циклическое расширение поля K, σ — образующий элемент группы Галуа поля E над полем K.*

а) *Для элемента $x \in E$ равенство $N_{E/K}(x) = 1$ имеет место в том и только в том случае, когда существует ненулевой элемент $y \in E$, для которого $x = y^{1-\sigma}\left(= y/\sigma^{-1}(y)\right)$. Каждый элемент $y_1 \in E$, для которого $x = y_1^{1-\sigma}$, имеет вид λy, где $\lambda \in K^*$;*

б) *для элемента $x \in E$ равенство $\mathrm{Tr}_{E/K}(x) = 0$ имеет место в том и только в том случае, когда существует элемент $z \in E$, для которого $x = z - \sigma(z)$. Каждый элемент $z_1 \in E$, для которого $x = z_1 - \sigma(z_1)$, имеет вид $z + \mu$, где $\mu \in K$.*

а) Пусть n — степень E над K. Для всякого элемента $t \in E$ построим элемент вида

$$u(t) = t + xt^{\bar{\sigma}} + x^{1+\bar{\sigma}}t^{\sigma^2} + x^{1+\sigma+\sigma^2}t^{\sigma^3} + \ldots + x^{1+\sigma+\ldots+\sigma^{n-2}}t^{\sigma^{n-1}}$$

поля E (резольвента Лагранжа — Гильберта). Поскольку n K-автоморфизмов σ^k $(0 \leqslant k \leqslant n-1)$ поля E линейно независимы (§ 10, теорема 3), существует элемент $t \in E$, для которого $y = u(t) \neq 0$. Для этого значения t, в силу соотношения $N_{E/K}(x) = x^{1+\sigma+\ldots+\sigma^{n-2}+\sigma^{n-1}} = 1$, имеем

$$y^{\sigma} = t^{\sigma} + x^{\sigma}t^{\sigma^2} + \ldots + x^{\sigma+\sigma^2+\ldots+\sigma^{n-2}}t^{\sigma^{n-1}} + tx^{-1},$$

откуда $xy^{\sigma} = y$, $x = y^{1-\sigma}$. Наоборот, очевидно, что из $x = y^{1-\sigma}$ следует, что $N_{E/K}(x) = 1$. Наконец, из соотношения $y^{1-\sigma} = y_1^{1-\sigma}$ вытекает $y_1 y^{-1} = (y_1 y^{-1})^{\sigma}$. Следовательно, элемент $y_1 y^{-1}$ инвариантен при всех K-автоморфизмах поля E, так что $y_1 y^{-1} \in K$ (§ 10, определение 1).

б) Известно (§ 10, предложение 10), что существует элемент $v \in E$, для которого $\mathrm{Tr}_{E/K}(v) \neq 0$. Рассмотрим элемент

$$Z = \frac{1}{\mathrm{Tr}_{E/K}(v)} (x\sigma(v) + (x + \sigma(x))\sigma^2(v) + \ldots + (x + \sigma(x) + \ldots + \sigma^{n-2}(x))\sigma^{n-1}(v)).$$

Если $\mathrm{Tr}_{E/K}(x) = \sum_{k=0}^{n-1} \sigma^k(x) = 0$, то

$$\sigma(Z) = \frac{1}{\mathrm{Tr}_{E/K}(v)} (\sigma(x)\sigma^2(v) + \ldots + (\sigma(x) + \sigma^2(x) + \ldots + \sigma^{n-2}(x))\sigma^{n-1}(v) - xv),$$

откуда следует, что $z - \sigma(z) = x$. Обратно: очевидно, что из равенства $x = z - \sigma(z)$ следует, что $\mathrm{Tr}_{E/K}(x) = 0$. Наконец, из соотношения $z - \sigma(z) = z_1 - \sigma(z_1)$ вытекает $z_1 - z = \sigma(z_1 - z)$. Таким образом, элемент $(z_1 - z)$ инвариантен при всех K-автоморфизмах поля E, следовательно, принадлежит полю K.

Следствие. *Пусть p — простое число, m и n — два произвольных целых положительных числа, $q = p^n$. Каждый ненулевой элемент конечного поля F_q является нормой некоторого элемента расширения F_{q^m} поля F_q. Каждый элемент поля F_q является следом некоторого элемента поля F_{q^m}.*

Действительно, поле F_{q^m} является циклическим расширением поля F_q, группа Галуа которого порождается автоморфизмом $x \to x^q$ (предложение 5). Найдем порядок подгруппы G (мультипликативной) группы F_q^*, являющейся образом $F_{q^m}^*$ при представлении $x \to N(x)$. G изоморфна факторгруппе группы $F_{q^m}^*$ по подгруппе U, состоящей из элементов x, для которых $N(x) = 1$. Но по теореме 3 подгруппа U является образом группы $F_{q^m}^*$ при представлении $y \to y^{q-1}$. Таким образом, группа U изоморфна факторгруппе группы $F_{q^m}^*$ по подгруппе, образованной теми элементами y, для которых $y = 1$. Но эти элементы y являются в точности элементами группы F_q^* (n° 3). Поэтому группа U имеет порядок, равный $(q^m - 1)/(q - 1)$. Следовательно, группа G имеет порядок $q - 1$, а потому совпадает с F_q^*.

Подобным же образом найдем порядок подгруппы H аддитивной группы F_q, являющейся образом группы F_{q^m} при отображении $x \to \mathrm{Tr}(x)$. Она изоморфна факторгруппе группы F_{q^m} по подгруппе V, состоящей из элементов x, для которых $\mathrm{Tr}(x) = 0$. По теореме 3 группа V является образом группы F_{q^m} при отображении (§ 1, предложение 1) $z \to z - z^q$. Таким образом, она изоморфна факторгруппе группы F_{q^m} по подгруппе, состоящей из элементов z, для которых $z = z^2$, то есть (n° 3) по подгруппе F_q. Порядок группы V равен, таким образом, q^m/q, следовательно, порядок группы H равен q, что доказывает совпадение H с F_q.

6. *Циклические расширения и двучленные уравнения*

Первая часть теоремы 3 позволяет описать простой способ образования некоторых циклических расширений поля K.

Предложение 6. *Пусть K — поле характеристики p, E — циклическое расширение поля K, степень n которого не делится на p, и пусть поле K содержит поле корней n-й степени из единицы. В этом случае существует неприводимый многочлен из кольца $K[X]$ вида $X^n - a$ такой, что поле E порождается произвольным корнем θ этого многочлена. Кроме того,*

ненулевой элемент $\xi \in E$ является корнем многочлена из кольца $K[X]$ вида $X^n - b$ в том и только в том случае, если $\xi = \lambda\theta^k$, где k — целое число, а $\lambda \in K$. Более сильное условие $E = K(\xi)$ имеет место в том и только в том случае, если числа k и n взаимно просты и $\lambda \neq 0$.

Действительно, пусть $\zeta \in K$ — примитивный корень n-й степени из единицы. Имеем $N_{E/K}(\zeta) = \zeta^n = 1$. Таким образом, существует элемент $\theta \in E$, для которого $\zeta = \theta^{1-\sigma}$ или, иначе, $\sigma(\theta) = \zeta\theta$. Из этого видно, что $\sigma^k(\theta) = \zeta^k\theta$. Следовательно, θ имеет n различных сопряженных, другими словами, имеет степень n над полем K, откуда $E = K(\theta)$. С другой стороны, имеем $1 = \zeta^n = (\theta^n)^{1-\sigma}$, то есть $\sigma(\theta^n) = \theta^n$. Это доказывает, что $\theta^n \in K$. Если $\xi \in E$ и $\xi^n = b \in K$, то имеем $\sigma(\xi^n) = \xi^n$, откуда $(\xi^{1-\sigma})^n = 1$. Таким образом, $\sigma(\xi) = \omega\xi$, где ω — какой-то корень из единицы. Если $\omega = \zeta^{-k} = (\theta^{\sigma-1})^k$, то получим $\sigma(\xi\theta^{-k}) = \xi\theta^{-k}$, откуда $\xi\theta^{-k} \in K$. Обратно, если $\xi = \lambda\theta^k$, где $\lambda \in K$ и k — целое число, то имеем $\xi^n = \lambda^n(\theta^n)^k = \lambda^n a^k \in K$. Если, кроме того, $E = K(\xi)$, то n сопряженных $\sigma^h(\xi) = \omega^h\xi$ $(0 \leqslant h \leqslant n-1)$ элемента ξ должны быть различными элементами (§ 7, n° 7). Но это и означает, что ω является примитивным корнем n-й степени из единицы. Следовательно (лемма 1), числа k и n взаимно просты.

Алгебраическое уравнение вида $x^n - a = 0$ называется «двучленным уравнением».

Предложение 6 допускает следующее обращение:

Предложение 7. *Пусть K — поле характеристики p, n — целое число, не кратное p, для которого поле K содержит поле корней n-й степени из единицы в поле Ω. Для любого элемента $a \in K^*$ поле корней E многочлена $X^n - a$ является циклическим расширением поля K, и порождается произвольным корнем многочлена $X^n - a$. Степень $[E : K] = d$ является делителем числа n и равна наименьшему целому числу $r > 0$, для которого a^r является n-й степенью элемента поля K.*

Действительно, пусть θ — корень многочлена $X^n - a$. Для любого другого корня θ' этого многочлена имеем $(\theta'/\theta)^n = 1$. Отсюда $\theta' = \omega\theta$, где ω — корень n-й степени из единицы, который принадлежит полю K по предположению. Таким образом, $\theta' \in K(\theta)$, что доказывает равенство $E = K(\theta)$. Поскольку производная nX^{n-1}

многочлена $X^n - a$ обращается в нуль лишь при $x = 0$, все корни многочлена $X^n - a$ просты (за исключением случая $a = 0$. Этот тривиальный случай мы оставляем в стороне). Таким образом (§ 10, следствие предложения 6), поле E является расширением Галуа поля K. Пусть Γ — группа Галуа поля E над K, σ — произвольный элемент группы Γ. Поскольку $E = K(\theta)$, задание $\sigma(\theta)$ определяет σ (§ 6, n° 2). Но $\sigma(\theta)$ является корнем многочлена $X^n - a$. Следовательно, $\sigma(\theta) = \zeta_\sigma \theta$, где ζ_σ — корень n-й степени из единицы, вполне определяемый заданием σ. Отображение $\sigma \to \zeta_\sigma$ осуществляет взаимно однозначное соответствие между группой Γ и подгруппой мультипликативной группы G корней n-й степени из единицы. Кроме того, оно является *представлением* группы Γ в группу G, так как при $\tau \in \Gamma$ имеем

$$\sigma\tau(\theta) = \sigma(\tau(\theta)) = \sigma(\zeta_\tau \theta) = \zeta_\tau \sigma(\theta) = \zeta_\sigma \zeta_\tau \theta,$$

где

$$\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau.$$

Итак, видим, что группа Γ изоморфна *подгруппе* группы G. Поскольку G — циклическая группа порядка n (теорема 1), то Γ — циклическая группа, порядок d которой делит n. Положим $n = dh$. Из соотношений $\sigma(\theta) = \zeta_\sigma \theta$ для $\sigma \in \Gamma$ вытекает, что $N_{E/K}(\theta) = \mu\theta^a$, где $\mu \in K$, откуда $\theta^d = b \in K$. Следовательно, имеем $a = \theta^n = b^h$, откуда $a^d = b^{dh} = b^n$. Если бы существовало число $r < d$, для которого $a^r = c^n$, где $c \in K$, то из соотношения $\theta^n = a$ следовало бы, что $\theta^{rn} = c^n$, откуда $\theta^r = \omega c$, где ω — корень n-й степени из единицы. Таким образом, элемент θ был бы корнем многочлена $X^r - \omega c$ из кольца $K[X]$, в противоречии с тем, что θ имеет степень d над полем K.

Если поле K не содержит поле корней n-й степени из единицы, то предложения 6 и 7 перестают быть верными (см. упражнение 7 и § 6, упражнение 7).

Упражнения. 1) а) Доказать, что поле $R_n(F_q)$ корней n-й степени из единицы в алгебраическом замыкании конечного поля F_q (n не кратно характеристике p поля F_q) совпадает с полем F_{q^m}, где m — наименьшее из целых чисел, для которых $q^m - 1$ кратно n. Вывести из этого, что многочлен Φ_n неприводим в кольце $F_q[X]$ в том и только в том случае, если класс, содержащий q, в группе обратимых элементов кольца $Z/(n)$ имеет порядок, равный $\varphi(n)$.

б) Вывести из а), что для каждого простого числа p, не являющегося делителем 12, многочлен $\Phi_{12}(X)$ приводим в каждом из колец $F_p[X]$. В этом случае F_p содержит всегда корни 12-й степени из единицы, отличные от нее самой.

в) Доказать, что поле F_3 не содержит ни одного корня 13-й степени из единицы, отличного от 1. Но степень поля $R_{13}(F_3)$ над F_3 равна 3, что меньше, чем $\varphi(13)=12$.

г) Пусть $q=p^m$; доказать, что в кольце $F_q[X]$ многочлен $X^{q^n}-X$ равен произведению всех унитарных неприводимых многочленов, степени которых делит n (использовать предложение 3). Пусть h_i $(1\leqslant i\leqslant r)$—различные простые делители числа n. Доказать, что число элементов $\zeta\in F_{q^n}$, для которых $F_{q^n}=F_q(\zeta)$, равно

$$\nu=q^n-\sum_i q^{\frac{n}{h_i}}+\sum_{i<j} q^{\frac{n}{h_ih_j}}-\sum_{i<j<k} q^{\frac{n}{h_ih_jh_k}}+\ldots+(-1)^r q^{\frac{n}{h_1h_2\ldots h_r}}.$$

(Заметить, что такой элемент характеризуется свойством не принадлежать ни к какому из полей вида $F_{q^{\frac{n}{h_i}}}$.) Доказать, что

$$q^n-\sum_i q^{\frac{n}{h_i}}\leqslant\nu\leqslant q^n-q^{\frac{n}{h_1h_2\ldots h_r}}.$$

Разобрать случай, где n—степень некоторого простого числа.

Вывести из этого подсчета значение числа унитарных неприводимых многочленов степени n в кольце $F_q[X]$.

3) Пусть ζ—примитивный корень $(q-1)$-й степени из единицы в поле F_q, так что любой элемент группы F_q^* представляется в виде ζ^k $(0\leqslant k\leqslant q-1)$. Доказать, что m-ми степенями элементов группы F_q^* являются элементы (в количестве $(q-1)/d$) вида ζ^{hd} $(0\leqslant h<(q-1)/d)$, где d—наибольший общий делитель чисел $q-1$ и m. Каждый из этих элементов является m-й степенью d различных элементов поля F_q.

4) В поле F_q $(q=p^n,\ p\neq 2)$ число ν решений (x_1, x_2) уравнения $a_1x_1^2+a_2x_2^2=b$ $(a_1a_2\neq 0)$ задается следующими формулами:

1° если $b=0$, а $-a_1a_2$ не является квадратом элемента в поле F_q, то $\nu=1$;

2° если $b\neq 0$, а $-a_1a_2$ не является квадратом элемента в поле F_q, то $\nu=q+1$;

3° если $b=0$, а $-a_1a_2$—квадрат некоторого элемента в поле F_q, то $\nu=2q-1$;

4° если $b\neq 0$, а $-a_1a_2$—квадрат некоторого элемента в поле F_q, то $\nu=q-1$.

(Если $-a_1a_2$ — квадрат, свести уравнение к виду $yz=c$.

Если $-a_1a_2$ не является квадратом, присоединить к полю F_q корень многочлена $X^2+a_1a_2$ и привести уравнение к виду $t^{q+1}=d$ в поле F_{q^2}, где $d\in F_q$. При этом использовать упражнение 3.)

5) а) В поле F_q ($q=p^n$, $p\neq 2$) число ν решений $(x_1, x_2, \ldots, x_{2m})$ уравнения

$$a_1x_1^2+a_2x_2^2+\ldots+a_{2m}x_{2m}^2=b\ (a_1a_2\ldots a_{2m}\neq 0)$$

задается следующими формулами:

1° если $b=0$, $a(-1)^m a_1a_2\ldots a_{2m}$ не является квадратом, то

$$\nu=q^{2m-1}-q^m+q^{m-1};$$

2° если $b\neq 0$, $a(-1)^m a_1a_2\ldots a_{2m}$ не является квадратом, то

$$\nu=q^{2m-1}+q^{m-1};$$

3° если $b=0$, $a(-1)^m a_1a_2\ldots a_{2m}$ — квадрат, то

$$\nu=q^{2m-1}+q^m-q^{m-1};$$

4° если $b\neq 0$, $a(-1)^m a_1a_2\ldots a_{2m}$ — квадрат, то

$$\nu=q^{2m-1}-q^{m-1}.$$

(Провести индукцию по m, использовав упражнение 4.)

б) Число ν решений уравнения

$$a_1x_1^2+a_2x_2^2+\ldots+a_{2n+1}x_{2n+1}^2=b\ (a_1a_2\ldots a_{2m+1}\neq 0)$$

задается следующими формулами:

1° если $b=0$, то

$$\nu=q^{2m};$$

2° если $b\neq 0$ и $(-1)^m a_1a_2\ldots a_{2m+1}b$ не является квадратом, то

$$\nu=q^{2m}-q^m;$$

3° если $b\neq 0$, а $(-1)^m a_1a_2\ldots a_{2m+1}b$ — квадрат, то

$$\nu=q^{2m}+q^m.$$

(Свести к случаю а).)

6) Пусть E — некоторое циклическое расширение поля K. Доказать, что E изоморфно тензорному произведению циклических расширений поля K, степени которых равны степеням некоторых простых чисел (использовать теорему 1 из § 10).

7) Пусть K — поле характеристики p, q — ненулевое простое число, для которого поле K содержит корни q-й степени из единицы. Пусть ζ — примитивный корень q-й степени из единицы.

а) Пусть E — циклическое расширение поля K степени q^e, σ — K-автоморфизм поля E, порождающий группу Галуа поля E над полем K. Пусть F_{e-1} — промежуточное поле между полями K и E степени q над полем K. В этом случае существует элемент $\theta\in E$,

являющийся корнем неприводимого многочлена $X^q - a_m$ из кольца $F[X]$, для которого $E = F(\theta)$ и $\theta^\sigma = \zeta\theta$ (где $m = q^{e-1}$). Доказать, что $E = K(\theta)$, $\theta^\sigma = \beta\theta$, где $\beta \in F$, причем $\alpha^{\sigma-1} = \beta^q$ и $N_{F/K}(\beta) = \zeta$. (Заметить, что по предложению 6 $\theta^\sigma = \beta\theta^k$ при $0 < k < q$ и $\beta \in F$. Вычислив $\theta^{\sigma^{mq}}$, доказать, что $k^{mq} - 1 \equiv 0 \pmod q$. Отсюда вывести, что $k = 1$.)

б) Обратно, пусть F — циклическое расширение поля K степени q^{e-1}. Пусть σ — K-автоморфизм поля F, порождающий группу Галуа поля F над полем K. Пусть существует элемент $\beta \in F$, для которого $N_{F/K}(\beta) = \zeta$, и пусть элемент $\alpha \in F$ таков, что $\alpha^{\sigma-1} = \beta^q$; доказать, что для любого элемента $\lambda \in K^*$ многочлен $X^q - \lambda\alpha$ неприводим в кольце $F[X]$. (Использовать при этом предложение 7.) Пусть θ — один из корней этого многочлена. Доказать существование K-изоморфизма $\bar{\sigma}$ поля $E = F(\theta)$ в поле Ω, продолжающего σ, причем $\theta^{\bar{\sigma}} = \beta\theta$. Вывести отсюда, что E является циклическим расширением поля K степени q^e, причем $\bar{\sigma}$ порождает группу Галуа поля E над K и $E = K(\theta)$. Доказать, наконец, что каждое циклическое расширение поля K степени q^e, содержащее поле F, является полем корней многочлена $X^q - \lambda\alpha$ из кольца $F[X]$ при соответствующем выборе элемента $\lambda \in K^*$ (применить теорему 3).

в) Рассмотреть в качестве поля K поле Q рациональных чисел. Многочлен $X^2 + 1$ неприводим в кольце $Q[X]$. Если i — один из его корней, то $F = Q(i)$ является циклическим расширением поля Q степени 2, но при этом не существует никакого циклического расширения поля Q степеяи 4, содержащего F.

*8) Пусть K — поле характеристики $p > 0$.

а) Пусть E — циклическое расширение степени p поля K. Доказать существование такого неприводимого многочлена в кольце $K[X]$ вида $X^p - X - a$, что поле E порождается произвольным корнем θ этого многочлена. (Заметить, что $\mathrm{Tr}_{E/K}(1) = 0$.) Элемент ξ порождает поле E и является корнем многочлена вида $X^p - X - b$ из кольца $K[X]$ в том и только в том случае, если $\xi = k\theta + \lambda$, где k — некоторое ненулевое целое число, а $\lambda \in K$.

б) Обратно, доказать, что при любом $a \in K$ многочлен $X^p - X - a$ либо неприводим в кольце $K[X]$, либо все его корни принадлежат полю K. В первом случае доказать, что поле корней E этого многочлена является циклическим расширением поля K степени p и порождено произвольным корнем многочлена $X^p - X - a$. (Рассуждать, как в предложении 7.)

*9) Пусть K — поле характеристики $p > 0$.

а) Пусть E — циклическое расширение поля K степени p^e, σ — K-автоморфизм поля E, порождающий группу Галуа поля E над полем K. Пусть F — промежуточное поле между полями E и K, степень которого над полем K равна p^{e-1}. Если $m = p^{e-1}$, то

существует корень $\theta \in E$ неприводимого многочлена $X^p - X - \alpha$ из кольца $F[X]$, для которого $E = F(\theta)$ и $\sigma^m(\theta) = \theta + 1$ (упражнение 8а)). Доказать, что при этом также $E = K(\theta)$ и $\sigma(\theta) = \theta + \beta$, где элемент $\beta \in F$ таков, что $\sigma(\alpha) - \alpha = \beta^p - \beta$ и $\mathrm{Tr}_{E/K}(\beta) = 1$.

б) Обратно, пусть F — циклическое расширение поля K степени p^{e-1} ($e > 1$), σ — K-автоморфизм поля F, порождающий группу Галуа поля F над полем K. Доказать существование двух элементов α, β из поля F, для которых $\mathrm{Tr}_{F/K}(\beta) = 1$ и $\sigma(\alpha) - \alpha = \beta^p - \beta$. (Использовать предложение 10 из § 10 и теорему 3 из § 11.) Вывести отсюда, что при любом $\lambda \in K$ многочлен $X^p - X - \alpha - \lambda$ неприводим в кольце $F[X]$ (см. упражнение 8б)). Пусть θ — корень этого многочлена. Доказать существование K-изоморфизма $\bar{\sigma}$ поля $E = F(\theta)$ в поле Ω, продолжающего σ, для которого $\bar{\sigma}(\theta) = \theta + \beta$. Заключить отсюда, что поле E является циклическим расширением поля K степени p^e, σ порождает группу Галуа поля E над полем K и $E = K(\theta)$. Доказать, наконец, что каждое циклическое расширение поля K степени p^e, содержащее поле F, является полем корней многочлена $X^p - X - \alpha - \lambda$ из кольца $F[X]$ при подходящем λ из поля K.

10) Пусть K — поле характеристики p, n — некоторое целое число (не делящееся на p), для которого поле K содержит все корни n-й степени из единицы. Пусть K_0 — подполе поля K, для которого K — расширение Галуа поля K_0. Пусть α — элемент поля K, для которого поле корней E многочлена $X^n - a$ имеет степень, равную n, над полем K. Поле E является расширением Галуа поля K_0 в том и только в том случае, если для любого K_0-автоморфизма τ поля K существуют целое число $r > 0$ и элемент $b \in K$, для которых $\tau(a) = b^n a^r$. (Использовать предложение 6.)

*11) Пусть K — поле характеристики p, n — целое число, которое не делится на p и для которого поле K содержит все корни n-степени из единицы. Пусть P_n — подгруппа мультипликативной группы K^* ненулевых элементов поля K, состоящая из n-х степеней элементов группы K^*. Пусть G — подгруппа группы K^*, содержащая P_n. Доказать, что из конечности индекса $(G : P_n)$ вытекает, что поле W (полученное присоединением к полю K всех корней многочленов $X^n - a$, где a пробегает группу G) является абелевым расширением поля K, степень которого конечна и равна $(G : P_n)$. Группа Галуа поля W над полем K изоморфна группе G/P_n (разложить группу G/P_n в прямое произведение циклических групп, провести индукцию по числу групповых сомножителей, используя предложение 7, предложение 6, упражнение 10, как и теорему 1 из § 10).

*12) Пусть K — поле характеристики p, n — целое число, не кратное p. Многочлен вида $X^n - a$ из кольца $K[X]$ неприводим в том и только в том случае, если для любого простого делителя q

числа n элемент a не равен q-й степени какого-либо элемента поля K и, кроме того, при $n \equiv 0 \pmod 4$, если a непредставим в виде $-4c^4$, где $c \in K$. (Доказательство достаточности условий при помощи упражнения 1, § 7 свести к случаю, когда $n = q^e$ (q простое); затем, определив с помощью упражнения 1 из § 7 вид свободного члена каждого неприводимого сомножителя многочлена $X^{q^e} - a$, провести индукцию по e.)

13) Пусть N — расширение Галуа конечной степени поля K, Γ — его группа Галуа над полем K. Пусть $(x_\sigma)_{\sigma \in \Gamma}$ — семейство ненулевых элементов из поля N. Для того чтобы выполнялись соотношения $x_{\sigma\tau} = x_\sigma x_\tau^\sigma$ для произвольных элементов σ и τ группы Γ, необходимо и достаточно существование ненулевого элемента $z \in N$, для которого $x_\sigma = z^{1-\sigma}$ при любых $\sigma \in \Gamma$. (Образовать элемент $z = \sum_{\sigma \in \Gamma} x_\sigma t^\sigma$, где $t \in N$.) Доказать, что этот результат содержится как частный случай теоремы 3, если группа Γ циклическая.

14) Пусть K — конечное тело, не обязательно *коммутативное*, Z — его центр, q — число элементов поля Z, n — ранг тела K над полем Z.

а) Доказать, что для любого подполя E поля K, содержащего поле z, ранг E над полем Z является делителем n.

б) Пусть $x \in K$ — элемент, не лежащий в центре Z. Доказать, что число различных сопряженных элементов yxy^{-1} для элемента x в группе K^* равно $(q^n - 1)/(q^d - 1)$, где d делит n и отлично от n. (Рассмотреть в K множество элементов, перестановочных с x, и использовать а).)

в) Вывести из б), что $q - 1$ делится на целое число $\Phi_n(q)$ (разложить группу K^* на классы сопряженных элементов и использовать тождество (2).)

г) Доказать, что при $n > 1$ имеем $\Phi_n(q) > (q-1)^{\varphi(n)}$ (разложить многочлен $\Phi_n(X)$ в поле комплексных чисел C). Вывести отсюда что $K = Z$, другими словами, что тело K *коммутативно*.

ПРИЛОЖЕНИЕ 1

К ГЛАВЕ V

СИММЕТРИЧЕСКИЕ РАЦИОНАЛЬНЫЕ ДРОБИ

1. Симметрические функции

Пусть K — поле, $N = K(X_1, X_2, \ldots, X_n)$ — поле рациональных дробей от n переменных над полем K. Для любой рациональной дроби $f \in N$ и любой перестановки σ из симметрической группы $\mathfrak{S}_n$ определим рациональную дробь σf следующим образом:

$$\sigma f(X_1, X_2, \ldots, X_n) = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})$$

(см. гл. III, § 5, n° 1). Очевидно, отображение $f \longrightarrow \sigma f$ является автоморфизмом поля N (гл. IV, § 3, предложение 2). Обозначим его символом φ_σ; отображение $\sigma \longrightarrow \varphi_\sigma$ является изоморфизмом группы $\mathfrak{S}_n$ в группу автоморфизмов поля N. Впредь мы будем отождествлять группу $\mathfrak{S}_n$ с ее образом при этом изоморфизме.

Симметрической рациональной дробью или, допуская вольность речи, *симметрической функцией* от X_i $(1 \leqslant i \leqslant n)$ назовем рациональную дробь $f \in N$, которая *инвариантна* относительно группы $\mathfrak{S}_n$ (т. е. $\sigma f = f$ для всех $\sigma \in \mathfrak{S}_n$) (см. гл. III, § 5, определение 2). Совокупность симметрических функций E является полем инвариантов группы $\mathfrak{S}_n$. Таким образом (§ 10, теорема 2), N является расширением Галуа поля E степени $n!$, группа Галуа которого совпадает с $\mathfrak{S}_n$. Очевидно, $N = E(X_1, X_2, \ldots, X_n)$. Рассмотрим в кольце $N(Z)$ многочлен

$$h(Z) = \prod_{i=1}^{n} (Z - X_i) = Z^n + \sum_{k=1}^{n} (-1)^k s_k z^{n-k},$$

где

$$s_k(X_1, X_2, \ldots, X_n) = \sum_{i_1<i_2<\ldots<i_k} X_{i_1}X_{i_2} \ldots X_{i_k}$$

для $1 \leqslant k \leqslant n$. Так как $h(Z) = \prod_{i=1}^{n}(Z - X_{\sigma(i)})$, любой перестановкой $\sigma \in \mathfrak{S}_n$ многочлен h не меняется при применении σ к его коэффициентам. Иначе говоря, коэффициенты s_k являются симметрическими функциями от X_i. Симметрическую функцию s_k называют *элементарной симметрической функцией степени* k от X_i ($1 \leqslant i \leqslant n$, $1 \leqslant k \leqslant n$). Таким образом, $s_k \in E$ для $1 \leqslant k \leqslant n$. Сейчас мы увидим, что E совпадает с полем $E' = K(s_1, s_2, \ldots, s_n)$. Действительно, N является полем корней многочлена $h \in E'[Z]$. Так как корни этого многочлена простые, то N является расширением Галуа поля E', его группа Галуа над полем E' является подгруппой группы $\mathfrak{S}_n$ (§ 10, n° 3). Из включений $E' \subset E \subset N$ вытекает, что $E = E'$.

Заметим еще, что так как поле N алгебраично над полем E, E и N имеют одну и ту же алгебраическую размерность над полем K (§ 5, теорема 4). Следовательно (§ 5, следствие 1 к теореме 1), элементы $s_1, s_2, \ldots, s_n$ образуют чистый базис поля E над полем K. Итак:

Предложение 1. *Для каждой симметрической рациональной дроби g из поля $K(X_1, X_2, \ldots, X_n)$ существует, и притом единственная рациональная дробь φ из поля $K(Z_1, Z_2, \ldots, Z_n)$, для которой*

$$g(X_1, X_2, \ldots, X_n) = \varphi(s_1, s_2, \ldots, s_n).$$

Пусть $f(Z) = Z^n + \sum_{k=1}^{n}(-1)^k a_k Z^{n-k}$ — произвольный унитарный многочлен из кольца $K[Z]$ степени n, Ω—алгебраическое замыкание поля K. Многочлен f разлагается в кольце $\Omega[Z]$ в произведение $\prod_{i=1}^{n}(Z - \alpha_i)$ многочленов первой степени, не обязательно различных. В этом случае имеем $a_k = s_k(\alpha_1, \ldots, \alpha_n)$ для $1 \leqslant k \leqslant n$. Если семейство элементов $(a_k)_{1 \leqslant k \leqslant n}$ допускает подстановку в рациональную дробь $\varphi(Z_1, \ldots, Z_n)$, то семейство элементов $(\alpha_k)_{1 \leqslant k \leqslant n}$ допускает подстановку в дробь $g(X_1, \ldots, X_n)$, причем $g(\alpha_1, \ldots, \alpha_n) = \varphi(a_1, \ldots, a_n)$ (гл. IV, § 3, предложение 3).

Ввиду алгебраической независимости над полем K элементов s_k из доказательства предложения 1 вытекает

Предложение 2. *Пусть K — произвольное поле, U_k $(1 \leqslant k \leqslant n)$ n-переменных. Многочлен $h(Z) = Z^n + U_1 Z^{n-1} + \ldots + U_{n-1} Z + U_n$ неприводим и сепарабелен над полем $E = K(U_1, U_2, \ldots, U_n)$. Поле N корней многочлена $h(Z)$ является расширением Галуа поля E, группа Галуа которого изоморфна симметрической группе $\mathfrak{S}_n$. Кроме того, поле N является чисто трансцендентным расширением поля K.*

2. *Симметрические многочлены*

Любую симметрическую рациональную дробь $g \in K(X_1, \ldots, X_n)$ можно записать в виде частного двух *симметрических* многочленов. Действительно, пусть $g = u/v$ (u, v — многочлены); положим $w = \prod_{\sigma \in \mathfrak{S}_n} (\sigma v)$; w является симметрическим многочленом, дробь w/v_1 есть некоторый многочлен v_1, причем $g = (uv_1)/w$. Из соотношения $uv_1 = gw$ вытекает, что uv_1 — симметрический многочлен, поскольку g и w — симметрические дроби.

Таким образом, симметрические многочлены образуют подкольцо P в поле E симметрических рациональных дробей; для этого кольца E является полем отношений. Мы сейчас уточним предложение 1 для симметрических многочленов.

Рассмотрим симметрический многочлен

$$f(X_1, \ldots, X_n) = \sum_{M} c_M M,$$

где M пробегает множество $\mathscr{M}$ одночленов от $X_1, \ldots, X_n$. Из соотношений $\sigma f = f$ при каждой перестановке $\sigma \in \mathfrak{S}_n$ вытекает, что равенство $c_{\sigma(M)} = c_M$ имеет место для любого одночлена M и любой перестановки $\sigma \in \mathfrak{S}_n$. В любом классе интранзитивности группы $\mathfrak{S}_n$, рассматриваемой как группа операторов на множестве одночленов $\mathscr{M}$, выберем некоторый (в остальном произвольный) одночлен. Пусть $\mathscr{P}$ — множество этих одночленов. Для каждого одночлена $M \in \mathscr{P}$ пусть Γ_M — подгруппа групп $\mathfrak{S}_n$, оставляющая инвариантным одночлен M. Пусть q — ее индекс в группе $\mathfrak{S}_n$. В каждом левом смежном классе группы $\mathfrak{S}_n$ по подгруппе

Γ_M возьмем по перестановке $\sigma_j (1 \leqslant j \leqslant q)$. Пусть $\tau(M) = \sum_{j=1}^{q} \sigma_j M$. Таким образом, $\tau(M)$ можно определить и как сумму всех *различных* одночленов в семействе $n!$ одночленов вида σM ($\sigma \in \mathfrak{S}_n$). Из этого вытекает тотчас, что $\tau(M)$ является *симметрическим* многочленом и что $f = \sum_{M \in \mathcal{P}} c_M \tau(M)$. Кроме того, ясно, что многочлены $\tau(M)$ *линейно независимы* над полем K, когда M пробегает множество $\mathcal{P}$. Таким образом, они образуют *базис* алгебры P симметрических многочленов (над полем K).

Предложение 3. *Для любого одночлена* M (относительно $X_1, X_2, \ldots, X_n$) *существует многочлен* $\varphi(Y_1, Y_2, \ldots, Y_n)$ *с целыми рациональными коэффициентами, для которого* $\tau(M) = \varphi(s_1, s_2, \ldots, s_n)$.

Рассмотрим *градуировку* (гл. IV, § 1, n° 3) кольца $Z[Y_1, Y_2, \ldots, Y_n]$, в которой *вес* одночлена $Y_1^{\lambda_1} Y_2^{\lambda_2} \ldots Y_n^{\lambda_n}$ по определению примем равным $\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n$. При этом соглашении мы сейчас уточним результат, сформулированный в предложении 3, доказав существование многочлена φ, вес которого равен *полной степени* k одночлена M и такого, что $\tau(M) = \varphi(s_1, s_2, \ldots, s_n)$. Сначала проведем индукцию по n. Предложение очевидно при $n = 1$. С другой стороны, для фиксированного n предложение очевидно при $k = 0$. Мы проведем также индукцию по k.

Положим $\tau(M) = f(X_1, X_2, \ldots, X_n)$. Многочлен $f(X_1, X_2, \ldots, X_{n-1}, 0)$ симметрический, причем все его ненулевые коэффициенты равны 1.

В силу предположения индукции существует многочлен $\varphi_1 \times (Y_1, \ldots, Y_{n-1})$ с целыми рациональными коэффициентами, вес которого не превосходит k и для которого

$$f(X_1, \ldots, X_{n-1}, 0) = \varphi_1(s'_1, \ldots, s'_{n-1}).$$

Здесь $s'_h(X_1, \ldots, X_{n-1}) = s_h(X_1, \ldots, X_{n-1}, 0)$ является элементарной симметрической функцией степени h от X_i с $i \leqslant n-1$ $(1 \leqslant h \leqslant n-1)$. Рассмотрим симметрический многочлен

$$f_1(X_1, \ldots, X_{n-1}, X_n) = f(X_1, \ldots, X_{n-1}, X_n) - \varphi_1(s_1, \ldots, s_{n-1}),$$

коэффициенты которого целые рациональные числа. Поскольку вес φ_1 не превосходит k, полная степень многочлена f_1 также

не превосходит k. С другой стороны, $f_1(X_1, \ldots, X_{n-1}, 0) = 0$. Следовательно, все члены многочлена f_1 содержат в качестве множителя X_n. Но так как f_1 — симметрический многочлен, то переменные $X_1, \ldots, X_{n-1}$ также являются множителями в каждом из членов многочлена f_1. Поэтому можем написать $f_1(X_1, \ldots, X_n) = s_n g(X_1, \ldots, X_n)$, где g — симметрический многочлен с целыми рациональными коэффициентами, а его полная степень $\leqslant k-n < k$. В силу индуктивного предположения существует многочлен $\varphi_2(Y_1, \ldots, Y_n)$, веса $\leqslant k-n$, с целыми коэффициентами, для которого $g(X_1, \ldots, X_n) = \varphi_2(s_1, \ldots, s_n)$, откуда

$$f(X_1, \ldots, X_n) = \varphi_1(s_1, \ldots, s_{n-1}) + s_n\varphi_2(s_1, \ldots, s_n) = \varphi(s_1, \ldots, s_n).$$

Вес многочлена φ не превосходит k. Пусть его вес $<k$; тогда полная степень многочлена f также будет $< k$. Следовательно, вес многочлена φ равен k, что заканчивает доказательство.

Заметим, что предыдущие рассмотрения позволяют определить симметрические многочлены в *любой* алгебре многочленов $\Delta[X_1, X_2, \ldots, X_n]$ над *произвольным* коммутативным кольцом с единицей.

3. *Формула Ньютона*

Мы поставим себе целью получить рекуррентные формулы («формулы Ньютона»), позволяющие вычислять выражения симметрических многочленов

$$p_k(X_1, X_2, \ldots, X_n) = X_1^k + X_2^k + \ldots + X_n^k \ (k \geqslant 0)$$

в виде многочленов от $s_1, s_2, \ldots, s_n$.

Предложение 4. *Имеем*

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \ldots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0 \quad (1)$$

для $1 \leqslant k \leqslant n$ *и*

$$p_k - p_{k-1}s_1 + \ldots + (-1)^{n-1} p_{k-n+1}s_{n-1} + (-1)^n p_{k-n}s_n = 0 \quad (2)$$

для $k > n$.

Первое доказательство. Пусть $f(Z) = (Z-X_1)(Z-X_2)\ldots(Z-X_n)$ (в кольце $N[Z]$, где $N = K(X_1, \ldots, X_n)$); тогда

$$\frac{f'(Z)}{f(Z)} = \sum_{i=1}^{n} \frac{1}{Z-X_i}. \quad (3)$$

Но разложение $1/(Z-X_i)$ в формальный степенной ряд по $1/Z$ (гл. IV, § 5, предложение 5) имеет вид $\frac{1}{Z}+\frac{X_i}{Z^2}+\frac{X_i^2}{Z^3}+\ldots+\frac{X_i^k}{Z^{k+1}}\ldots$ Следовательно, уравнение (3) записывается в виде

$$\frac{f'(Z)}{f(Z)}=\frac{n}{Z}+\frac{p_1}{Z^2}+\frac{p_2}{Z^3}+\ldots+\frac{p_k}{Z^{k+1}}+\ldots$$

или, умножая обе части на $f(Z)/Z^n$,

$$n-(n-1)\frac{s_1}{Z}+(n-2)\frac{s_2}{Z^2}+\ldots+(-1)^{n-1}\frac{s_{n-1}}{Z^{n-1}}=$$
$$=\left(1-\frac{s_1}{Z}+\frac{s_2}{Z^2}+\ldots+(-1)^n\frac{s_n}{Z^n}\right)\left(n+\frac{p_1}{Z}+\ldots+\frac{p_k}{Z^k}+\ldots\right). \tag{4}$$

Достаточно теперь сравнить коэффициенты при $1/Z^k$ в двух частях равенства (4), чтобы получить формулы (1) и (2).

Второе доказательство. Из соотношений

$$X_i^n-s_1X_i^{n-1}+s_2X_i^{n-2}+\ldots+(-1)^{n-1}s_{n-1}X_i+(-1)^n s_n=0$$

для $1\leqslant i\leqslant n$ следует при $k\geqslant n$

$$X_i^k-s_1X_i^{k-1}+\ldots+(-1)^{n-1}s_{n-1}X_i^{k-n+1}+$$
$$+(-1)^n s_nX_i^{k-n}=0\ (1\leqslant i\leqslant n).$$

Складывая эти n соотношений, мы получим тождество (2). Для доказательства соотношения (1) мы используем следующую лемму:

Лемма. *Пусть K — поле, f — однородный многочлен степени $q<n$ из кольца $K[X_1, X_2, \ldots, X_n]$. Если многочлен f обращается в нуль при подстановке нуля в произвольные $n-q$ из n переменных $X_i\ (1\leqslant i\leqslant n)$, то $f=0$.*

Действительно, если $f\neq 0$, то f является суммой ненулевых членов вида $aX_{i_1}^{\nu_1}\ldots X_{i_m}^{\nu_m}$, где $\nu_k\geqslant 1$ при $1\leqslant k\leqslant m$ и $\sum_{k=1}^{m}\nu_k=q$. Это доказывает, что $m\leqslant q$. Подставив нуль вместо тех элементов X_j, индексы которых отличны от индексов i_k, элементов, входящих в один из этих членов, мы получим, таким образом, ненулевой многочлен, что противоречит предположению.

Доказав лемму, рассмотрим симметрический многочлен

$$f(X_1, \ldots, X_n) = \\ = p_k - p_{k-1}s_1 + p_{k-2}s_2 + \ldots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k$$

для некоторого индекса $k < n$. Это однородный многочлен степени k. Далее

$$f(X_1, \ldots, X_k, 0, \ldots, 0) = \\ = p'_k - p'_{k-1}s'_1 + \ldots + (-1)^{k-1} p'_1 s'_{k-1} + (-1)^k k s'_k,$$

где

$$s'_j = s_j(X_1, \ldots, X_k, 0, \ldots, 0)$$

и

$$p'_j = p_j(X_1, \ldots, X_k, 0, \ldots, 0) = \sum_{i=1}^{k} X_i^j.$$

Поскольку s'_j — элементарная симметрическая функция степени j от $X_1, X_2, \ldots, X_k$, из формулы (1) (доказанной выше) для $n = k$ вытекает, что $f(X_1, \ldots, X_k, 0, \ldots, 0) = 0$. Так как f — симметрический многочлен, он обращается в нуль при подстановке нуля в произвольные $n - k$ из n переменных X_i $(1 \leqslant i \leqslant n)$, откуда, применяя лемму, получим $f = 0$.

Следствие. *Пусть K — поле характеристики нуль, $(\alpha_i)_{1 \leqslant i \leqslant n}$ и $(\beta_i)_{1 \leqslant i \leqslant n}$ — два семейства из n элементов поля K, для которых $\sum_{i=1}^{n} \alpha_i^k = \sum_{i=1}^{n} \beta_i^k$, где $1 \leqslant k \leqslant n$. При этих условиях существует перестановка σ множества $[1, n]$, для которой $\beta_i = \alpha_{\sigma(i)}$, где $1 \leqslant i \leqslant n$.*

Действительно, формулы (1) доказывают индукцией по k, что $s_k(\alpha_1, \ldots, \alpha_n) = s_k(\beta_1, \ldots, \beta_n)$ (деление на произвольное целое число возможно в силу предположений относительно поля K). Следовательно, многочлены $\prod_{i=1}^{n}(X - \alpha_i)$ и $\prod_{i=1}^{n}(X - \beta_i)$ совпадают.

Упражнения. 1) Пусть K — произвольное поле, $N = K(X_1, \ldots, X_n)$ — поле рациональных дробей от n переменных над полем K, E — подполе поля K, образованное симметрическими рациональными дробями. Доказать, что элемент X_k $(1 \leqslant k \leqslant n)$ имеет степень $n - k + 1$ над полем $E(X_1, \ldots, X_{k-1})$. Какой многочлен играет роль его минимального многочлена над этим полем? Вывести отсюда,

что многочлен f из кольца $E[Z_1, Z_2, \ldots, Z_h]$ степени $\leqslant n-k$ относительно каждого из Z_j, для которого $f(X_1, X_2, \ldots, X_h)=0$, является нулевым.

2) Пусть f — симметрический многочлен из кольца $K[X_1, \ldots, X_n]$, φ — единственный многочлен из кольца $K[Y_1, \ldots, Y_n]$, для которого $f(X_1, \ldots, X_n)=\varphi(s_1, \ldots, s_n)$. Доказать, что полнан степень многочлена φ равна степени многочлена f относительно произвольной из переменных X_i.

3) В обозначениях предложения 4 положим $u_j=(-1)^{j+1}s_j$ $(1\leqslant j\leqslant n)$. Доказать, что

$$p_k=\sum a_{\lambda_1\lambda_2\ldots\lambda_n}u_1^{\lambda_1}u_2^{\lambda_2}\ldots u_n^{\lambda_n},$$

где суммирование ведется по всем системам $(\lambda_1, \ldots, \lambda_n)$ неотрицательных целых чисел, для которых $\lambda_1+2\lambda_2+\ldots+n\lambda_n=k$. Коэффициент $a_{\lambda_1\lambda_2\ldots\lambda_n}$ равен

$$\frac{k(\lambda_1+\lambda_2+\ldots+\lambda_n-1)!}{\lambda_1!\,\lambda_2!\ldots\lambda_n!}.$$

(Разложить $f'(Z)/f(Z)$ в формальный рнд по степеням $1/Z$, записав $f(Z)=Z^n-g(Z)$ и разложив сначала $1/f$ в ряд по степеням g/Z^n.)

4) Пусть K — поле характеристики нуль. Пусть α_i $(1\leqslant i\leqslant n)$ — n элементов из полн K, для которых $\alpha_1^k+\alpha_2^k+\ldots+\alpha_n^k=0$ при n последовательных значениях h, $h+1$, $\ldots$, $h+n-1$ индекса k. Доказать, что в этом случае $\alpha_1=\alpha_2=\ldots=\alpha_n=0$. Показать на примере, что это уже на так, если n значений индекса k не является последовательными числами или если поле K имеет характеристику, отличную от нулн.

*5) Пусть K — произвольное поле, f — рациональная дробь из поля $K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$. Обозначим символом σf (σ — любая перестановка из $\mathfrak{S}_n$) рациональную дробь

$$\sigma f(X_1, \ldots, X_n, Y_1, \ldots, Y_n)=$$
$$=f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}).$$

Говорят, что f — *симметрическая* рациональная дробь относительно пар (X_i, Y_i), если $\sigma f=f$ при любых $\sigma\in\mathfrak{S}_n$.

а) Для любого элемента $\nu=(\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n)$ из N^{2n} и любой перестановки $\sigma\in\mathfrak{S}_n$ положим

$$\sigma^{-1}(\nu)=(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}, \mu_{\sigma(1)}, \ldots, \mu_{\sigma(n)}).$$

Группу $\mathfrak{S}_n$, тем самым, можно рассматривать в качестве группы операторов в N^{2n} (гл. I, § 7, n° 3). Пусть γ — произвольный класс

интранзитивности группы $\mathfrak{S}_n$ в N^{2n}. Обозначим символом u_γ симметрический многочлен

$$\sum X_1^{\lambda_1} X_2^{\lambda_2} \dots X_n^{\lambda_n} Y_1^{\mu_1} \dots Y_n^{\mu_n},$$

где $(\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n)$ пробегает множество γ.

Доказать, что многочлены u_γ образуют базис (над полем K) векторного пространства симметрических многочленов относительно пар (X_i, Y_i).

б) Предположим, что характеристика поля K равна нулю. Доказать, что любой многочлен u_γ равен некоторому многочлену с рациональными коэффициентами относительно симметрических функций

$$v_{\lambda\mu} = \sum_{i=1}^{n} X_i^\lambda Y_i^\mu.$$

(Вести доказательство индукцией по числу пар (λ_i, μ_i), отличных от (0, 0) в строке $\nu = (\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n)$. Рассмотреть произведения $u_\gamma v_{\lambda\mu}$.)

в) *Элементарными* симметрическими функциями от (X_i, Y_i) будем называть $n(n+3)/2$ многочленов вида $w_{hk} = u_\gamma$, соответствующих классам интранзитивности γ элементов $(\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n)$, отличных от $(0, \dots, 0)$ и для которых h пар имеют вид (λ_i, μ_i) $(1, 0)$, k других пар — $(0, 1)$, а $n-h-k$ остальных — $(0, 0)$. Доказать (при условии, что характеристика поля K равна нулю), что любой симметрический многочлен относительно (X_i, Y_i) равен некоторому многочлену с коэффициентами в поле K относительно элементарных симметрических функций. (Рассмотреть суммы вида $\sum_{i=1}^{n} (UX_i + VY_i)^k$, где U и V — две переменные. Использовать б).)

г) Пусть K — поле характеристики 3 и $n \geqslant 4$, доказать, что многочлен $\sum_{i=1}^{n} X_i^2 Y_i^2$ не равен никакому многочлену с коэффициентами из поля K относительно симметрических функций w_{hk}.

ПРИЛОЖЕНИЕ II

К ГЛАВЕ V

РАСШИРЕНИЯ ГАЛУА БЕСКОНЕЧНОЙ СТЕПЕНИ

1. Топологическая группа Галуа

Пусть K — поле, N — расширение Галуа поля K, Γ — группа Галуа поля N над полем K. Если N — расширение *бесконечной* степени над полем K, то уже не существует взаимно однозначного соответствия между подгруппами группы Γ и промежуточными полями между полями K и N. Точнее говоря, может существовать подгруппа Δ группы Γ, отличная от Γ, но имеющая в качестве поля инвариантов то же, что и у Γ поле K (упражнение 1). Все же следующее предложение справедливо.

Предложение 1. *Пусть N — расширение Галуа поля K, Γ — группа Галуа поля N над K, Δ — подгруппа группы Γ, поле инвариантов которой совпадает с полем K. Для любого подрасширения L поля N, являющегося расширением Галуа поля K и имеющего над ним конечную степень, любой K-автоморфизм поля L является ограничением автоморфизма, принадлежащего группе Δ.*

Действительно, ограничения на L автоморфизмов $\sigma \in \Delta$ образуют некоторую группу K-автоморфизмов поля L (§ 6, предложение 6), поле инвариантов которой совпадает с полем K. Поскольку поле L имеет конечную степень над полем K, эта группа совпадает с группой Галуа поля L над полем K (§ 10, теорема 2).

Мы сейчас переформулируем результат предложения 1 на топологическом языке. Для любого подрасширения L поля N, являющегося расширением Галуа и имеющего *конечную* степень

над полем K, пусть $g(L)$ — группа Галуа поля N над полем L (подгруппа группы Γ, образованная из автоморфизмов $\sigma \in \Gamma$, оставляющих инвариантным каждый элемент поля L). Множества $g(L)$ образуют *базис фильтра* на Γ, ибо для двух расширений Галуа L и M поля K, содержащихся в N и имеющих конечные степени, $K(L \cup M)$ является расширением Галуа конечной степени над полем K (§ 10, предложение 5).

С другой стороны, подгруппы $g(L)$ являются *нормальными делителями* в группе Γ (§ 10, предложение 4). Таким образом, они определяют на Γ топологию, *согласованную* со структурой группы Γ. В этой топологии они образуют *фундаментальную систему* окрестностей единичного элемента ε (Общ. топол., гл. III, § 1, n° 2). В дальнейшем, рассматривая группу Галуа некоторого расширения Галуа произвольного поля K, мы всегда будем подразумевать (если не оговорено противное), что эта группа наделена выше определенной топологией.

Тогда предложение 1 можно выразить в следующей эквивалентной форме:

Предложение 2. *Пусть N — расширение Галуа поля K, Γ — группа Галуа поля N над полем K. Подгруппа Δ группы Γ, поле инвариантов которой совпадает с полем K, всюду плотна в группе Γ.*

Действительно, для любого элемента $\sigma \in \Gamma$ и любого расширения Галуа $L \subset N$ поля K конечной степени над полем K существует элемент $\tau \in \Delta$, для которого ограничения элементов σ и τ на L, в силу предложения 1, совпадают. Следовательно, $\sigma^{-1}\tau \in g(L)$, откуда следует предложение.

2. *Свойства топологических групп Галуа*

Пусть N — расширение Галуа поля K, Γ — его группа Галуа, $L \subset N$ — расширение Галуа конечной степени поля K. Для двух элементов τ, σ группы Γ имеем $\sigma^{-1}\tau \in g(L)$ в том и только в том случае, если $\sigma(x) = \tau(x)$ для всех элементов x некоторой системы образующих поля L над полем K, которую, в силу предположения, можно выбрать конечной. Наоборот, поскольку всякое расширение Галуа поля K, порожденное конечною частью поля N, имеет конечную степень над полем K (§ 6, следствие 1 к пред-

ложению 9), мы видим, что топология группы Γ является в точности *топологией простой сходимости*. Предполагается при этом, что поле N наделено *дискретной* топологией (Общ. топол., гл. X, § 1, n° 3). Можно добавить, что при рассмотрении группы Γ в качестве части множества N^N отображений из N в N ее топология индуцируется топологией *произведения* дискретных топологий на сомножителях в N^N.

Если N наделить равномерной дискретной топологией, то группа Γ является equicontinu. Это заново доказывает, что топология простой сходимости согласуется со структурой группы Γ (Общ. топол., гл. X, § 3, предложение 11).

Предложение 3. *Группа Галуа* Γ *расширения Галуа поля* K *является вполне несвязной компактной группой.*

Действительно, Γ как подпространство пространства N^N отделимо и вполне несвязно, как все пространство N^N (Общ. топол., гл. I, § 11, предложение 9). Для любого элемента $x \in N$ множество элементов вида $\sigma(x)$, где σ пробегает группу Γ, *конечно*, поскольку оно является множеством сопряженных над полем K к алгебраическому над полем K элементу x. Все проекции группы Γ на пространства сомножителей произведения N^N являются конечными множествами. Это доказывает относительную компактность группы Γ в N^N (Общ. топол., гл. I, § 10, следствие к теореме 2). Остается лишь доказать *замкнутость* Γ в N^N. Но если u принадлежит к замыканию Γ в N^N, то для любой пары (x, y) точек из N существует элемент $\sigma \in \Gamma$, для которого $\sigma(x) = u(x)$, $\sigma(y) = u(y)$, $\sigma(x+y) = u(x+y)$ и $\sigma(xy) = u(xy)$. Отсюда следует, что $u(x+y) = u(x) + u(y)$ и $u(xy) = u(x)\,u(y)$. Это доказывает, что u является эндоморфизмом поля N. Для всякого элемента $x \in K$ подобными же рассуждениями покажем, что $u(x) = x$. Таким образом, u является K-эндоморфизмом поля N, а в силу алгебраичности поля N над K u является, следовательно, и K-автоморфизмом поля N (§ 6, предложение 4).

То обстоятельство, что группа Γ вполне несвязна, вытекает также и из того, что для любого подрасширения L поля N, являющегося расширением Галуа конечной степени над полем K, подгруппа $g(L)$ группы Γ, которая, по определению, есть

окрестность нуля, *открыта* в Г. Следовательно, она также и *замкнута* (Общ. топол., гл. III, § 2, предложение 4). Более общо:

Предложение 4. *Пусть N — расширение Галуа поля K, Γ — его группа Галуа. Если F — подрасширение поля N конечной степени над полем K, то группа Галуа $g(F)$ поля N над полем F является подгруппой, одновременно открытой и замкнутой в группе* Г.

Действительно, пусть L — расширение Галуа, порожденное F; L имеет конечную степень над полем K (§ 6, следствие 1 к предложению 9), причем $g(L) \subset g(F)$. Следовательно, единичный элемент группы Г является внутренней точкой подгруппы $g(F)$, что и доказывает предложение (Общ. топол., гл. III, § 2, предложение 4).

Рассмотрим теперь *произвольное* подрасширение E поля N. Группа Галуа $g(E)$ поля N над полем E является множеством элементов $\sigma \in \Gamma$, для которых $\sigma(x) = x$ для любого $x \in E$. Поскольку любая из проекций $\sigma \to \sigma(x)$ группы Г на пространства сомножителей в N^N непрерывна, $g(E)$ является *замкнутой* подгруппой группы Г (Общ. топол., гл. I, § 8, следствие предложения 6). Топология группы Г индуцирует на $g(E)$ топологию простой сходимости в N. Таким образом, индуцированная топология совпадает с топологией, определенной на группе Галуа $g(E)$ методом n° 1.

Обратно, рассмотрим произвольную подгруппу Δ группы Г. Пусть $E = k(\Delta)$ — поле инвариантов группы Δ. В силу предложения 2 подгруппа Δ *всюду плотна* в группе Галуа $g(E)$, которая является, следовательно, *замыканием* подгруппы Δ в группе Г. В итоге основная теорема о расширениях Галуа конечной степени (§ 10, теорема 3) обобщается следующим образом:

Теорема 1. *Пусть N — расширение Галуа поля K, Γ — его (топологическая) группа Галуа. Пусть $\mathfrak{K}$ — множество промежуточных полей между полями K и N, пусть $\mathfrak{G}$ — множество замкнутых подгрупп группы* Г. *Для любой подгруппы $E \in \mathfrak{G}$ пусть $k(\Delta)$ — поле инвариантов группы Δ. Для любого подполя $E \in \mathfrak{K}$ пусть $g(E)$ — группа Галуа поля N над E. Отображение $E \to g(E)$ является взаимно однозначным отображением из $\mathfrak{K}$ на $\mathfrak{G}$, для которого $\Delta \to k(\Delta)$ является обратным отображением.*

Предложение 5. *Пусть N — расширение Галуа поля K, E — расширение Галуа поля K, содержащееся в поле N. Пусть Γ — группа Галуа поля N над полем K, Δ — группа Галуа поля N над полем E. Группа Галуа поля E над полем K изоморфна (топологической) группе Γ/Δ.*

Поскольку группы Галуа полей N и E относительно поля K компактны, все сводится к доказательству того, что отображение $\sigma \to \sigma_E$ (которое каждому автоморфизму $\sigma \in \Gamma$ ставит в соответствие его ограничение на E) является *непрерывным* на Γ (§ 10, предложение 4 и Общ. топол., гл. I, § 10, теорема 1). Но если L — некоторое подрасширение поля E, являющееся расширением Галуа конечной степени относительно поля K, то из включения $\sigma \in g(L)$ следует, что σ_E содержится в группе Галуа поля E относительно поля L. Отсюда следует предложение.

Упражнения. 1) а) Пусть N — расширение Галуа поля K бесконечной степени над K. Доказать, что группа Галуа Γ поля N над K *не является счетной* (используя упражнение 18 из § 8, построить множество K-автоморфизмов поля N мощности континуум).

б) Вывести из этого, что в этом случае в группе Γ существуют незамкнутые подгруппы (рассмотреть счетные подгруппы группы Γ).

2) Пусть Ω — расширение поля K, N — подрасширение поля Ω, являющееся расширением Галуа поля $\mathscr{K}$, E — произвольное подрасширение поля Ω. Доказать, что (топологическая) группа Галуа поля N над $E \cap N$ изоморфна (топологической) группе Галуа поля E (N) над E (использовать следствие 1 теоремы 1 из § 10).

3) Пусть N — расширение Галуа поля K, $(E_\iota)_{\iota \in I}$ — семейство подрасширений поля N, каждое из которых является расширением Галуа над K и для которых:

1° для любого индекса $\varkappa$, обозначая символом $E'_\varkappa$ поле, порожденное объединением E_ι с $\iota \neq \varkappa$, имеем $E_\varkappa \cap E'_\varkappa = K$;

2° поле N порождено объединением E_ι.

а) Доказать, что поле N изоморфно тензорному произведению $\bigotimes_{(I)} E_\iota$ расширений E_ι поля K (гл. III, Приложение I, п° 2) (определить изоморфизм этого произведения на N, использовав теорему 1 из § 10).

б) Пусть Γ_ι — группа Галуа поля E_ι относительно K; доказать, что (топологическая) группа Галуа поля N относительно K изоморфна произведению (топологических) групп Γ_ι.

4) Пусть N — расширение Галуа поля K, A — наибольшее абелево расширение поля K, содержащееся в N (§ 10, следствие предложения 5). Пусть Γ — группа Галуа поля N над K; доказать, что

группа Галуа поля N над A является замыканием коммутанта группы Г.

* 5) Пусть Ω_p—алгебраическое замыкание простого поля F_p. Для любого простого числа l пусть N_l—объединение расширений поля F_p, содержащихся в Ω_p, степени которых являются степенями числа l.

а) Доказать, что N_l является абелевым расширением поля F_p, группа Галуа Γ_l которого изоморфна (топологической) аддитивной группе Z_l целых l-адических чисел (определить изоморфизм из Z_l на Γ_l, используя при этом предложение 5 из § 11).

б) Доказать, что поле Ω_p является абелевым расширением поля F_p, что его группа Галуа Г изоморфна произведению топологических групп Z_l, где l пробегает множество простых чисел (см. упражнение 3). Доказать, что счетная подгруппа группы Г, порожденная автоморфизмом $x \to x^p$ всюду плотна в Г.

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВАМ IV И V

(Римские цифры относятся к библиографии, помещенной в конце этих замечаний.)

Теория полей, а также тесно связанная с ней теория многочленов — прямой продукт деятельности, составлявшей до середины XIX века основное содержание классической алгебры. Эта деятельность была направлена на решение алгебраических уравнений и сводящихся к ним задач о геометрических построениях.

Пытаясь решить алгебраическое уравнение выше первой степени, мы оказываемся перед совершенно новыми вычислительными трудностями, ибо становится невозможным определить значение неизвестной, пользуясь лишь «рациональными» действиями над данными задачами. Это затруднение, видимо, было обнаружено чрезвычайно давно. Одним из важнейших математических вкладов вавилонян следует считать то обстоятельство, что им удалось свести решение квадратных и биквадратных уравнений к единственной новой алгебраической операции: извлечению квадратных корней. (Это устанавливается дошедшими до нас текстами ((I), стр. 183—193), в которых таким способом решены многочисленные уравнения с числовыми коэффициентами.) Что касается разработки формального исчисления, античной науке так и не удалось продвинуться в задаче решения алгебраических уравнений дальше этого. В самом деле, греки классической эпохи лишь переоткрыли вавилонские формулы в геометрических терминах; использование этих результатов в алгебраическом виде засвидетельствовано не раньше Герона (100 г. н. э.) и Диофанта.

Решительный прогресс был достигнут греками в совершенно ином направлении. Мы почти не знаем, как вавилоняне представляли себе корни квадратные из целых чисел, не являющихся квадратами, и как они их вычисляли *). В немногочисленных дошедших до нас текстах по этому вопросу авторы, по-видимому, довольствуются довольно грубыми прибли-

*) Во всех примерах квадратных и биквадратных уравнений в вавилонских текстах данные подобраны так, что корни приходится извлекать из точных квадратов.

женными методами ((I), стр. 33—38). Пифагорейская школа, строго определившая понятие соизмеримых величин и придававшая этому понятию почти религиозный характер, не могла оставаться на этой точке зрения. Возможно, что именно безуспешность последовательных попыток рационально выразить число $\sqrt{2}$ привела к доказательству иррациональности этого числа *).

В другом месте (см. Исторические замечания к гл. IV Книги III) мы уже указывали, что это открытие, знаменующее решительный поворот в истории математических наук, оказало глубокое влияние на понятие «числа» у греков и привело их к созданию алгебры исключительно геометрического характера. Цель этого состояла в отыскании способа представления (или, быть может, доказательства «существования») несоизмеримых отношений, которые греки отказывались считать числами. Чаще всего они сводили алгебраическую задачу к нахождению пересечения двух вспомогательных плоских кривых, выбранных подходящим образом, или же к последовательному разысканию нескольких таких пересечений. Поздняя и не заслуживающая большого доверия традиция приписывает Платону первую классификацию этих конструкций, которой суждена долгая и блистательная история. По-видимому, по причинам скорее философского, чем математического, характера Платон специально выделил так называемые «построения циркулем и линейкой», т. е. те, в которых лишь прямые линии и окружности используются в качестве вспомогательных кривых **).

Во всяком случае, Евклид в своих «Началах» (II) ограничивается только задачами, разрешимыми этим способом (не называя их, впрочем, особым термином).

Это обстоятельство, безусловно, немало способствовало привлечению внимания к таким задачам математиков последующих веков. Теперь, одна-

---

*) Один современный автор высказал остроумное замечание о том, что построение правильного звездчатого пятиугольника, известное пифагорейцам (пятиугольник был у них одним из мистических символов), немедленно дает иррациональность числа $\sqrt{5}$. Он же предложил гипотезу (к сожалению, не подтвержденную никакими текстами) о том, что именно на этом пути пифагорейцы открыли иррациональные числа (K. von Fritz, Ann. of Math., t. XLVI, 242 (1945)).

**) В связи с этим Платону приписывается также разделение плоских кривых на «плоские» (прямая и окружность), «телесные» (конические сечения, получаемые как пересечение плоскости с твердым телом-конусом) и все остальные, объединенные общим названием «τόποι γραμμικοί». Любопытно, что влияние этой классификации прослеживается еще у Декарта, который в своей «Геометрии» относит к одному и тому же «роду» уравнения степени $2n - 1$ и $2n$: без сомнения потому, что уравнения первой и второй степени решаются перечислением «плоских» кривых, а уравнения третьей и четвертой степени — перечислением «телесных» кривых.

ко, мы знаем *), что алгебраические уравнения, которые можно решить «циркулем и линейкой», относятся к весьма специальному виду: в частности, неприводимое уравнение третьей степени (над полем рациональных чисел) нельзя решить таким способом. Между тем, греки уже давно встретились с подобными задачами, которым суждено было стать знаменитыми: удвоение куба (решение уравнения $x^3 = 2$) и трисекция угла. С другой стороны, квадратура круга поставила древних математиков перед лицом трансцендентной проблемы. Мы обнаруживаем, что для решения этих задач вводились многочисленные алгебраические кривые (конические сечения, циссоида Диоклеса, конхоида Никомеда) и трансцендентные кривые (квадратриса Динострата, спираль Архимеда). Это обстоятельство не могло не привести к изучению таких кривых самих по себе, что подготовило почву для будущего развития аналитической геометрии, алгебраической геометрии и исчисления бесконечно малых. Подобные методы, однако, не способствовали никакому прогрессу в решении алгебраических уравнений **).

Единственным трудом античности, содержащим значительный вклад в этот вопрос и долгое время влиявшим на алгебраистов средневековья и Возрождения, осталась книга X «Начал» Евклида (II). В этой книге (основные результаты которой некоторые историки склонны приписывать Теэтету) Евклид рассматривает выражения, получающиеся в результате комбинации нескольких радикалов, например $\sqrt{\sqrt{a} \pm \sqrt{b}}$ (a и b — рациональные числа). Он дает условия, при которых такие выражения иррациональны, разделяет

---

*) Отыскание точек пересечения прямой и окружности (или двух окружностей) равносильно решению уравнения второй степени, коэффициенты которого являются рациональными функциями от коэффициентов рассматриваемой прямой и окружности (или двух окружностей). Отсюда легко вывести, что координаты точки, которую можно построить «циркулем и линейкой», исходя из данных точек, принадлежат некоторому расширению L поля рациональных чисел Q, описываемому следующим образом. Пусть K — поле, полученное присоединением к Q координат заданных точек. Тогда существует возрастающая последовательность полей $(L_i)_{0 \leqslant i \leqslant n}$, промежуточных между K и L и удовлетворяющих условиям $K = L_0$, $L = L_n$, $[L_i : L_{i-1}] = 2$ при $1 \leqslant i \leqslant n$. Индукция по n показывает, что степень над полем K расширения Галуа N, порожденного расширением L, является *степенью двойки*. Можно доказать, что и наоборот, при выполнении последнего условия существует последовательность полей (L_i), промежуточных между K и L с описанными выше свойствами. Тогда поставленная задача решается циркулем и линейкой (ср. Н. Г. Чеботарев, Основы теории Галуа, Гостехиздат (1934), ч. I).

**) Из-за отсутствия удобного алгебраического исчисления у греков мы не находим каких-либо попыток классифицировать задачи, которые не удавалось решить «циркулем и линейкой». Арабы первыми свели многочисленные задачи этого рода (например, построение правильных семи- и девятиугольников) к решению кубических уравнений.

их на многочисленные категории (и доказывает, что эти категории не совпадают), а также изучает алгебраические соотношения между этими иррациональностями типа (в современной записи)

$$\sqrt{\sqrt{p}+\sqrt{q}}=\sqrt{\frac{1}{2}(\sqrt{p}+\sqrt{p-q})}+\sqrt{\frac{1}{2}(\sqrt{p}-\sqrt{p-q})}.$$

Все это выражено обычным геометрическим языком «начал», что делает изложение особенно тяжеловесным и неудобным.

После упадка классической греческой математики концепции, относящиеся к алгебраическим уравнениям, претерпевают изменения. Несомненно, что на протяжении всего классического периода греки владели методами сколь угодно точного вычисления квадратных корней. К сожалению, мы мало осведомлены об этом *).

У индусов, затем у арабов и их западных соперников средних веков извлечение корней любых порядков становится постепенно одной из основных операций наряду с рациональными операциями алгебры и, как эти последние, обозначается все более удобными для вычислений символами **). Теория уравнений второй степени, непрерывно совершенствуемая в продолжение всего средневековья (число корней, отрицательные корни, неразрешимый случай, двойные корни), а также теория биквадратных уравнений дают те образцы формул решения «в радикалах», которые алгебраисты нескольких веков будут пытаться перенести на уравнения высших степеней, в первую очередь кубические. Леонардо Пизанский, главный проводник арабской науки в Европе XIII века, во всяком случае, уже сознает, что иррациональности, расклассифицированные Евклидом в его десятой книге, не годятся для этой цели (новое доказательство невозможности в теории, которая изо-

---

*) Например, принадлежащий Архимеду метод приближенного вычисления числа π требует знания ряда квадратных корней с довольно большой точностью. Мы не знаем, однако, каким способом Архимед вычислял эти корни. Метод вычисления $\sqrt{2}$, доставляющий разложение этого числа в «непрерывную дробь», известен нам (в геометрической форме) из текста Теона Смирнейского (II в. н. э.); возможно, что он восходит к ранним пифагорейцам. Тот способ отыскания приближений к квадратным корням, который и в наши дни преподается в средней школе, засвидетельствован впервые у Теона Александрийского (IV в. н. э.), хотя, несомненно, он был известен уже Птоломею. Отметим, наконец, что у Герона (около 100 г. н. э.) можно найти приближенное вычисление одного кубического корня (ср. G. Enestrőm, Bibl. Math. (3), t. VIII, 412 (1907)).

**) Иррациональность числа $\sqrt[n]{a}$, где a — целое число, не являющееся точной n-й степенью, впервые отмечена и доказана Штифелем (XVI век). Впрочем, его доказательство скопировано с доказательства Евклида при $n = 2$, и представляется довольно маловероятным, чтобы такое нетрудное обобщение не было замечено раньше.

билует ими). Он пытается провести аналогичные вычисления с кубическими корнями и получает соотношения типа

$$\sqrt[3]{16}+\sqrt[3]{54}=\sqrt[3]{250},$$

подобные формулам Евклида для квадратных корней (впрочем, более ранние примеры таких тождеств засвидетельствованы у арабов). Все же пройдут еще три века бесплодных попыток, пока Сципион дель Ферро в начале XVI века не придет, наконец, к формуле решения уравнения $x^3 + ax = b$:

$$x=\sqrt[3]{\frac{b}{2}+\sqrt{\left(\frac{b}{2}\right)^2+\left(\frac{a}{3}\right)^3}}+\sqrt[3]{\frac{b}{2}-\sqrt{\left(\frac{b}{2}\right)^2+\left(\frac{a}{3}\right)^3}}. \qquad (1)$$

Не нам описывать здесь красочную историю этого сенсационного открытия — ссоры, вызванные им между Тартальей с одной стороны и Кардано и его школой с другой, или набрасывать портреты, порой весьма притягательные, ученых, оказавшихся в этом споре противниками. Но мы должны отметить решительные продвижения в теории уравнений, достигнутые Кардано и его учениками вследствие этого открытия.

Так, Кардано, пользовавшийся отрицательными числами охотнее, чем большинство его современников, замечает, что у кубических многочленов может быть три корня, а у биквадратных — четыре ((III), т. IV, стр. 259). Он отмечает, кроме того, что сумма трех корней уравнения $x^3 + bx = ax^2 + c$ (у которого, впрочем, член с x^2 уже умели уничтожать) всегда равна a (там же). Несомненно, руководствуясь этим соотношением и своей общей интуицией, он приходит к первоначальной идее о кратности корня. Он осмеливается даже (не без ораторских предостережений) производить формальные выкладки с выражениями, в которые входят квадратные корни из отрицательных чисел. Кажется правдоподобным, что к этому его привело естественное появление таких выражений в формуле (1) при $\left(\frac{b}{2}\right)^2+\left(\frac{a}{3}\right)^3<0$ (так называемый «случай неприводимости», в котором, как понял Кардано, уравнение имеет три вещественных корня). Это обстоятельство, во всяком случае, с очевидностью проявляется у его ученика Р. Бомбелли, который в своей «Алгебре» ((IV), стр. 293) доказывает соотношение

$$\sqrt[3]{2+\sqrt{-121}}=2+\sqrt{-1}$$

и заботится о том, чтобы дать правила действий над комплексными числами в явном виде, уже весьма близком к современным изложениям *).

*) Бомбелли ((IV), стр. 169 и 190) рассматривает комплексные числа как «линейные комбинации» с вещественными коэффициентами четырех базисных элементов: «piu» (+1), «meno» (−1), «piu de meno» (+i) и «meno di meno» (−i). В частности, он формулирует аксиому, согласно которой «piu» и «piu de meno» «не складываются»— первое появление понятия линейной независимости.

Наконец, в 1545 году другому ученику Кардано, Л. Феррари, удается решить общее уравнение четвертой степени с помощью вспомогательного кубического уравнения *).

Период, последовавший за эпохой столь быстрого прогресса и продлившийся вплоть до середины XVIII века, отмечен лишь развитием новых идей, введенных итальянской школой. Благодаря существенным усовершенствованиям, внесенным в систему алгебраических обозначений, Виета смог установить общие соотношения между коэффициентами и корнями любого алгебраического уравнения по крайней мере в случае, когда все корни положительны **) ((V), стр. 158). Более решительный А. Жирар, не колеблясь, утверждает (разумеется, без доказательства), что у всякого уравнения степени n имеется в точности n корней, если считать также «невозможные корни», каждый со своей кратностью и что эти корни удовлетворяют соотношениям, данным Виета. Он же впервые получает формулы для сумм одинаковых степеней корней вплоть до четвертой степени.

Но творческий дух XVII века обращен к иным целям, и Алгебре лишь перепадает кое-что из новейших открытий Аналитической геометрии и Исчисления бесконечно малых. Так, с методом Декарта проведения касательных к алгебраическим кривым (ср. Исторические замечания к Книге IV, гл. I, II, III) связан критерий кратности корня алгебраического уравнения, сформулированный учеником Декарта Гудде ((VIII), стр. 433 и 507—509). Несомненно, что также под влиянием Декарта начинается различение между алгебраическими и трансцендентными функциями, параллельное введенному в его «Геометрии» делению кривых на «геометрические» и «механические» (ср. Исторические замечания к Книге IV, гл. I, II, III). Это различение, во всяком случае, становится совершенно явным у Грегори, который в 1667 году пытается даже доказать, что площадь кругового сектора не может быть алгебраической функцией его хорды и радиуса ***).

Слово «трансцендентный» принадлежит Лейбницу, который всю жизнь интересовался подобными классификационными вопросами и который

---

*) Приведя первоначальное уравнение к виду $x^4 = ax^2 + bx + c$, стараются затем определить число z таким образом, чтобы правая часть уравнения

$$(x^2 + z)^2 = (a + 2z)\,x^2 + bx + (c + z^2)$$

была полным квадратом, что дает для z уравнение третьей степени.

**) Виета, страстный поклонник античности, систематически избегает использования отрицательных чисел в своих рассуждениях. Это не мешает ему при случае выражать на своем языке соотношения между коэффициентами и корнями, когда некоторые из последних отрицательны. Например, если у уравнения $x^3 + b = ax$ есть два положительных корня x_1, x_2 ($a > 0$, $b > 0$), Виета показывает, что $x_1^2 + x_2^2 + x_1x_2 = a$ и $x_1x_2\,(x_1 + x_2) = b$ ((V), стр. 106).

***) J. Gregory, Vera Circuli et Hyperbolae Quadratura..., Pataviae, 1667; ср. G. Heinrich, Bibl. Math. (3), t. II, 77—85 (1901).

в 1682 году открыл простое доказательство результата, не дававшегося Грегори, установив, что $\sin x$ не является алгебраической функцией от x ((VIII), т. V, стр. 97—98) *). Лейбниц и его друг Чирнгаузен, кроме того, были единственными математиками своего времени, еще интересовавшимися проблемой решения алгебраических уравнений «в радикалах». Мы видим, как в начале своей деятельности Лейбниц изучает «случай неприводимости» уравнения третьей степени и убеждается (впрочем, без достаточного доказательства), что в этом случае нельзя избавиться от мнимых величин в формулах для решений ((IX), стр. 547—564). Тогда же он безуспешно пытается решить в радикалах уравнение пятой степени. Когда позже Чирнгаузен утверждает, что он решил эту проблему, избавившись от всех членов уравнения, кроме двух крайних, с помощью преобразования вида $y = P(x)$, где P — подходящий многочлен четвертой степени, Лейбниц немедленно обнаруживает, что уравнения, определяющие коэффициенты многочлена $P(x)$, имеют степень >5, и оценивает этот метод как безнадежный ((IX), стр. 402—403).

По-видимому, именно нужды нового Анализа понемногу восстановили интерес к алгебре. Интегрирование рациональных дробей, осуществленное Лейбницем и Иоганном Бернулли, а также тесно связанный с этим вопрос о мнимых логарифмах, дают повод для углубления расчетов с комплексными числами и приводят к новой постановке вопроса о разложении многочлена на множители первой степени («основная теорема алгебры») **).

В начале XVIII века Котес и Муавр сводят решение двучленного уравнения $x^n - 1$ к делению окружности на n равных частей. Для выражения корней «в радикалах» поэтому оказывается достаточным найти соответствующие формулы для нечетного простого числа n. Муавр замечает, что в этом случае подстановка $y = x + \frac{1}{x}$ сводит задачу к решению «в радикалах» некоторого

*) Определение «трансцендентных величин» у Лейбница ((VIII), т. V, стр. 228; см. также стр. 120) применимо скорее к функциям, чем к числам (то, что он делает, на современном языке сводится к определению трансцендентных элементов над полем, полученным в результате присоединения данных задачи к полю рациональных чисел). Представляется правдоподобным, однако, что Лейбниц имел довольно четкое понятие о трансцендентных числах (хотя их точное определение, как будто, было дано не раньше конца XVIII века). Во всяком случае, Лейбниц в явном виде замечает, что трансцендентная функция может принимать рациональные значения при рациональных значениях аргумента и, следовательно, что его доказательство трансцендентности функции $\sin x$ еще недостаточно для доказательства иррациональности числа π ((VIII), т. V, стр. 97 и 124—126).

**) О зачаточном состоянии, в котором в то время находилось еще исчисление комплексных величин, можно составить себе отчетливое представление, читая Лейбница (одного из наиболее опытных в этом исчислении математиков той эпохи), который выражается так, как будто считает невозможным разложить многочлен $x^4 + 1$ на два вещественных множителя второй степени ((VIII), т. V, стр. 359—360).

уравнения степени $\frac{n-1}{2}$. Что до «основной теоремы», то после многократных неудач с общим решением «в радикалах» (включая несколько попыток Эйлера (X)) начинаются поиски априорных доказательств, не использующих явных формул для решений. Не входя в детали предлагавшихся методов (которые в конце концов привели к доказательствам Лагранжа и Гаусса; ср. Исторические замечания к Книге II, гл. VI, VII и Книге III, гл. VIII), отметим здесь точку зрения, с которой эта проблема рассматривается в середине XVIII века. Допускается (без какого бы то ни было оправдания, кроме смутного ощущения «общего случая», несомненно обязанного своим возникновением, как у А. Жирара, наличию соотношений между коэффициентами и корнями), что у всякого уравнения степени n есть n «идеальных» корней, с которыми можно вычислять, как с числами, *не зная, являются ли они числами* (вещественными или комплексными). Предполагается доказать (пользуясь правилами действий с этими идеальными корнями), что по крайней мере один из корней является обычным комплексным числом *).

В этом несовершенном виде можно различить уже первый росток общей идеи «формального присоединения», которой, несмотря на возражения Гаусса ((XIII), т. III, стр. 1), суждено было стать основой современной теории коммутативных полей.

С основоположными работами Лагранжа (XIa) и Вандермонда (XII) 1770 год открывает новый и решающий период в истории теории алгебраических уравнений. Безраздельно царившему до той поры эмпиризму более или менее удачных попыток найти формулы для решений приходит на смену систематический анализ поставленных проблем и методов, способных с ними справиться, — анализ, который через шестьдесят лет привел к окончательным результатам Галуа. Как Лагранж, так и Вандермонд исходят из неопределенности, к которой приводят разные значения радикалов в формулах для решения уравнений степени $\leqslant 4$. Это обстоятельство уже привлекало внимание Эйлера, который среди прочего показал, как следует согласовывать значения корней в формуле дель Ферро, чтобы получить 3 корня, а не 9. Лагранж замечает, что каждый из кубических радикалов в формуле дель Ферро можно записать в виде $\frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3)$, где ω — некоторый кубический корень из единицы, x_1, x_2, x_3 — три корня рассматриваемого уравнения, взятые в определенном порядке. Лагранж затем делает фундаментальное наблюдение, что функция $(x_1 + \omega x_2 + \omega^2 x_3)^3$ от трех корней может принимать лишь *два* разных значения при всевозможных перестановках корней, что *априорно* объясняет успех методов решения кубического уравнения. Подобный же анализ методов решения уравнения четвертой степени приводит к функции $x_1x_2 + x_3x_4$ четырех корней, принимающей только *три* разных значения при всевозможных перестановках корней и являющейся, стало быть, корнем

*) Следует отметить, что «мнимые (imaginaires) корни» математиков XVIII века — это часто именно «идеальные» корни, относительно которых и пытаются доказать, что они имеют вид $a + b\sqrt{-1}$ (см., например, (XIб)).

некоторого кубического уравнения, коэффициенты которого суть рациональные функции от коэффициентов первоначального уравнения *). Лагранж говорит, что эти факты «*составляют истинные принципы и, так сказать, саму метафизику* **) *разрешения в радикалах уравнений третьей и четвертой степени*» ((XI), стр. 357). Опираясь на эти примеры, Лагранж намеревается изучить в общем случае для уравнений степени n, какое количество ν разных значений ***) может принимать при произвольных перестановках корней рациональная функция V от этих корней. По существу, он закладывает тем самым (на языке, еще тесно связанном с теорией уравнений) основы теории групп и полей и получает несколько фундаментальных результатов этих теорий, используя те же принципы, которыми мы пользуемся сегодня. Например, он доказывает, что число ν делит $n!$, тем же рассуждением, которое служит сейчас для доказательства того факта, что порядок подгруппы конечной группы делит порядок всей группы. Еще более замечательная теорема, в которой он показывает, что если две рациональные функции от корней V_1 и V_2 остаются инвариантными при одних и тех же перестановках, то каждая из них является рациональной функцией от другой и от коэффициентов уравнения (частный случай теоремы Галуа, характеризующей всякое подрасширение расширения Галуа как поле инвариантов его группы Галуа). «*Эта проблема*,— говорит Лагранж,— *представляется мне одной из важнейших в теории уравнений, и ее общее решение, которое мы даем ниже, должно показать в новом свете эту часть Алгебры*» ((XI), стр. 374).

Все эти изыскания, естественно, в духе Лагранжа являются лишь подготовкой к анализу возможных методов решения алгебраических уравнений их последовательным сведением к уравнениям меньшей степени, ибо всякий такой метод, как показывает Лагранж, связан с образованием рациональных функций от корней, принимающих меньше n значений при всевозможных перестановках корней. Руководствуясь, несомненно, своими результатами о кубическом уравнении, он вводит в общем случае «резольвенты Лагранжа» $y_k = \sum_{h=1}^{n} \omega_k^h x_h$, где ω_k — корень n-й степени из единицы $(1 \leqslant k \leqslant h)$,

*) В этом слове, столь часто выходящем из-под пера авторов XVIII века, допустимо усматривать первый, еще довольно смутный зачаток современного понятия *структуры*.

**) Варинг также заметил это обстоятельство в своих «Алгебраических размышлениях», которые вышли в свет в том же 1770 году, но был не в состоянии извлечь из этого наблюдения те следствия, которые извлек из него Лагранж.

***) Лагранж уже проводит различие между различными *рациональными дробями*, которые получаются из V перестановками переменных x_i $(1 \leqslant i \leqslant n)$ и различными *значениями*, которые принимают эти дроби, когда x_i являются корнями некоторого алгебраического уравнения с данными численными коэффициентами. Все же его изложение не лишено колебаний по этому поводу, и лишь у Галуа это различие становится более явным.

с очевидностью показывает, как знание этих n чисел позволяет найти корни y_k, и вычисляет в общем случае степень уравнения, которому удовлетворяют числа y_k. Он показывает, например, что если n — простое число, то y_k являются корнями некоторого уравнения степени $n-1$, коэффициенты которого представляют собой рациональные функции одного корня уравнения степени $(n-2)!$; коэффициенты последнего рационально выражаются через коэффициенты первоначального уравнения. «*Если я не обманываюсь,— заключает он,— таковы истинные принципы разрешения уравнений и надлежащий анализ, который к ним приводит; как видно, все сводится к комбинаторному исчислению специального рода, которое позволяет априори находить ожидаемые результаты*» ((XIa), стр. 403).

Что касается мемуара Вандермонда, написанного независимо от работы Лагранжа, в нем имеются многочисленные точки соприкосновения с этой работой, в частности идея отыскивать рациональные функции от корней, принимающие по возможности мало разных значений при перестановках корней *), и изучение «резольвент Лагранжа», также введенных Вандермондом по этому поводу. Хотя его мемуар далеко не имеет ясности и общности, которые присущи труду Лагранжа, в одном пункте Вандермонд явно идет дальше Лагранжа, применяя все эти идеи к уравнению деления круга $x^n - 1$ при простых нечетных n. В то время как Лагранж ограничивается напоминанием о сведении этого уравнения к уравнению степени $m = \frac{n-1}{2}$ с рациональными коэффициентами и не пытается решить его при $n \geqslant 11$, Вандермонд утверждает, что m-е степени резольвент Лагранжа этого уравнения рациональны из-за соотношений между различными корнями уравнения $x^n - 1$; но основательность этого утверждения он проверяет лишь при $n = 11$, не доказывая его в общем случае.

Только тридцать лет спустя сформулированный Вандермондом результат был полностью доказан К. Ф. Гауссом **). Его окончательные результаты об уравнении $x^n - 1 = 0$ (n — простое нечетное число) находят свое место в общей программе его знаменитых арифметических исследований ((XIII), т. I, стр. 413 и далее) и особенно ярко иллюстрирует его мастерство в обращении с тем, что мы сегодня называем теорией циклических групп. Доказав, что многочлен $\frac{\Phi_n(x) = (x^n - 1)}{(x-1)}$ неприводим при всех нечетных

*) В этом исследовании (развитом в действительности лишь для уравнений пятой степени) впервые появляется понятие *импримитивности* ((XII), стр. 390—391). Кроме того, методы Лагранжа и Вандермонда естественно сближаются и с их работами того времени об определителях, благодаря которым идея перестановки и все, что с ней связано, должно было стать привычным этим ученым.

**) Гаусс не ссылается на Вандермонда в своих «Арифметических исследованиях», но правдоподобно, что он читал мемуар этого автора (ср. XIII, т. X, Abh. 4, стр. 58).

простых n *), Гаусс затем высказывает идею записать $n-1$ корней этого многочлена в виде $\zeta^{g^k} = \zeta_k$ $(0 \leqslant k \leqslant n-2)$, где g — примитивный корень сравнения $z^{n-1} \equiv 1 \bmod n$ (что на современном языке сводится к выяснению цикличности группы Г уравнения $\Phi_n(x) = 0$). Всякому делителю e числа $n-1$ Гаусс ставит в соответствие $f = (n-1)/e$ «периодов»

$$\eta_\nu = \zeta_\nu + \zeta_{\nu+e} + \zeta_{\nu+2e} + \ldots + \zeta_{\nu+(f-e)e} \qquad (1 \leqslant \nu \leqslant f)$$

и показывает, по существу, что линейные комбинации с рациональными коэффициентами чисел η_ν образуют поле, порожденное любым из f периодов η_ν и имеющее степень f над полем рациональных чисел (это поле, естественно, соответствует подгруппе порядка e группы Г). Здесь не место входить в детали этого анализа и важные арифметические следствия, из него происходящие. Укажем лишь, что он приводит, в частности, к знаменитой теореме о возможности строить «линейкой и циркулем» правильные многоугольники, число сторон которых — простое вида $2^{2^k}+1$ **).

Что до решения в радикалах уравнения $\Phi_n(x) = 0$, то оно легко получается из теории периодов в применении к f-й степени резольвенты Лагранжа $\sum_{\nu=0}^{f-1} \omega^\nu \eta_\nu$ (где $\omega^f = 1$) ***).

Непосредственно с работами Лагранжа связаны изыскания его соотечественника Руффини, одновременные с «Арифметическими исследованиями». Начиная с того, чем Лагранж кончил, Руффини провозглашает своей целью доказательство неразрешимости в «радикалах» «общего» ****) уравнения

---

*) Понятие неприводимого многочлена (с рациональными коэффициентами) восходит к XVII веку. Ньютон и Лейбниц уже описали способы, позволяющие (по крайней мере теоретически) определить неприводимые множители многочлена с данными рациональными коэффициентами ((VIII), т. IV, стр. 329 и 325), но результат Гаусса — первое доказательство неприводимости, применимое к целому *множеству* многочленов сколь угодно больших степеней.

**) Гаусс явно утверждает, что он может доказать, что это — единственный возможный случай построения циркулем и линейкой многоугольника с нечетным простым числом сторон ((XIII), т. I, стр. 462). Однако это доказательство никогда не было опубликовано и не найдено в его бумагах.

***) На самом деле, если хотеть доказать только разрешимость в радикалах, достаточно положить $e = 1$ и провести индукцию по n.

****) Математики XIX века понимают под этим, по существу, уравнение, коэффициентами которого являются *переменные* (indéterminées) над полем рациональных чисел. Но современное понятие переменной появляется не раньше последних лет XIX столетия. До тех пор под «многочленом» или «рациональной дробью» всегда понимали *функцию* комплексных переменных. «Общее» алгебраическое уравнение рассматривается как уравнение с независимыми комплексными переменными (variables) в качестве коэффициентов, корни которого суть «алгебраические функции» от этих переменных,—

пятой степени. Многословное и неясное доказательство Руффини осталось неполным, хотя и переделывалось несколько раз. Все же оно было уже очень близко к (в принципе верному) доказательству, позднее полученному Абелем *). Его главный интерес заключался во введении исчисления подстановок и первых понятий теории групп, которые Руффини развивает для доказательства несуществования функции от 5 корней уравнения, принимающей больше 2, но меньше 5 значений при всевозможных перестановках корней.

Мы уже описывали (Исторические замечания к гл. I), как несколько лет спустя Коши развил и систематизировал этот первый набросок теории групп перестановок. Но если в том, что касалось подстановок, понятия, необходимые для развития идей Лагранжа, постепенно прояснялись, основные принципы теории полей еще оставалось представить в столь же явном виде. Именно этого недоставало Руффини и именно это предстояло сделать Абелю и Галуа в последней фазе развития задачи о решении алгебраических уравнений.

Всю свою недолгую жизнь Абель не прекращает заниматься этой проблемой. Будучи еще почти ребенком, он думает, что получил формулу решения в радикалах уравнений пятой степени. Обнаружив позже свою ошибку, он не успокаивается, пока не находит доказательства того, что такой формулы не существует ((XIV), т. I, стр. 66). Но и на этом он не останавливается. Тогда как его соперник Якоби развивает теорию эллиптических функций как аналитик, в трудах Абеля на эту тему, посвященных теории уравнений деления эллиптических функций ((XIV), т. I, стр. 265, 377 et passim) доминирует алгебраическая точка зрения. Так, он получает новые типы разрешимых в радикалах уравнений методом, скопированным с метода Гаусса для уравнений деления круга ((XIV), т. I, стр. 310 и 358) **).

Исходя из этого, он поднимается до общего понятия «абелевых уравнений», разрешимость в радикалах которых доказывает в знаменитом мемуаре ((XIV), т. I, стр. 478). Именно в этой связи он вводит точное определение

понятие, лишенное поистине какого бы то ни было точного смысла, если слову «функция» придавать его современное значение. Разумеется, рассуждения, в которых фигурируют эти «алгебраические функции», в общем по существу верны, в чем можно убедиться, переводя их на современный алгебраический язык.

*) См. P. R u f f i n i, Opere Matematiche, v. 3, Roma (Ed. Cremonese), 1953—1954, а также H. B u r k h a r d t, Zeitschr. für Math. und Phys., XXXVII suppl., 121—129 (1892).

**) Гаусс в своих «Исследованиях» уже отмечал возможность обобщения его методов на уравнения деления лемнискаты ((XIV), т. I, стр. 413), и в делении на 5 ((XIII), т. X, стр. 161, 162 и 517). Как многие другие краткие и загадочные указания, которыми Гаусс по своей излюбленной привычке усеивал свои работы, соответствующая фраза из «Исследований» возбуждала воображение современников. Мы знаем, что она играла немалую побудительную роль для Абеля и Якоби в их исследованиях на эту тему.

неприводимости многочлена над данным полем (порожденным коэффициентами изучаемого уравнения *).

Смерть настигла его в 1829 году, когда он занимался общей проблемой описания всех уравнений, разрешимых в радикалах, и только что сообщил Креллю и Лежандру о своих результатах, уже весьма близких к будущим достижениям Галуа ((XIV), т. II, стр. 219—243, 269—270 и 279).

Именно Галуа довелось три года спустя завершить всю постройку (XV). Как и Абель, но с еще большей отчетливостью, он начинает с определений (с точностью до терминологии) принадлежности величины к полю, порожденному данными величинами; понятия присоединения; понятия многочленов, неприводимого над данным полем. Задавшись уравнением $F(x) = 0$ без кратных корней, с коэффициентами в данном поле K, Галуа последовательно показывает, что «*всегда можно образовать такую функцию V от корней, что все значения, принимаемые ею при всевозможных перестановках корней, будут разными*», что эта функция «*обладает тем свойством, что все корни первоначального уравнения рационально выражаются через V*», и наконец, обозначая через V, V', V'',... все корни неприводимого уравнения, которому удовлетворяет V, что «*если $a = f(V)$ — один из корней первоначального уравнения, то $f(V')$ также будет его корнем*» ((XV), стр. 36—37). Выражаясь современным языком, Галуа доказывает тем самым, что V, как и любая сопряженная к V величина, порождает поле N корней многочлена F. Затем он определяет группу Г уравнения $F = 0$ как множество тех перестановок корней x_i, которые получаются подстановкой всевозможных сопряженных к V в рациональные выражения корней x_i через V. После этого он немедленно устанавливает то фундаментальное обстоятельство, что элементы поля K характеризуются их инвариантностью при всех подстановках группы Г ((XV), стр. 38—39). Затем он доказывает, что если поле N содержит поле корней L другого многочлена, то группа поля N над L является нормальным делителем группы Г (понятие, специально введенное по этому поводу) ((XV), стр. 41 и 25—26). Отсюда он выводит, наконец, критерий разрешимости в радикалах с помощью рассуждения, существенные этапы которого состоят в следующем. Принимается, что основное поле K содержит все корни из единицы. Тогда, по предположению, должна существовать возрастающая последовательность полей $(K_i)_{0 \leqslant i \leqslant m}$, промежуточных между K и N, где мы положили $K_0 = K$, $K_m = N$ и где поле K_{i+1} получается присоединением к K_i всех корней двучленного уравнения $x^{n_i} - a_i = 0$ ($a_i \in K_i$). Следовательно, в группе Г существует такая убывающая последовательность (Γ_i) подгрупп, для которой $\Gamma_0 = \Gamma$, $\Gamma_m = \{\varepsilon\}$ (единичный элемент), Γ_{i+1} является нормальным делителем в Γ_i, а факторгруппы Γ_i/Γ_{i+1} цикличны (в этом случае

*) Само понятие поля (как и более общее понятие множества) остается почти чуждым математической мысли до Кантора и Дедекинда. Абель и Галуа определяют элементы своих «основных полей» как величины, рационально выражающиеся через заданные величины, но и не помышляют о рассмотрении в явном виде всего множества этих элементов.

группа Г называется *разрешимой*). Обратно, если это условие выполнено, использование подходящей резольвенты Лагранжа показывает, что поле K_{i+1} получается присоединением к K_i всех корней некоторого двучленного уравнения (ср. § 11, теорема 3) и, стало быть, уравнение $F(x) = 0$ разрешимо в радикалах *).

Невозможность решить в радикалах «общее» уравнение степени $n > 4$ следует тогда из того обстоятельства, что группа Г такого уравнения, изоморфная симметрической группе $\mathfrak{S}_n$ (Приложение I, n° 1), не является разрешимой (ср. гл. I, § 7, упражнение 11).

* * *

Как мы уже отмечали (ср. Исторические замечания к гл. I), начиная с середины XIX века, алгебранты значительно расширили область своих исследований, до тех пор почти исключительно посвященных изучению уравнений. В свете открытий Галуа становится ясным, что задача решения «в радикалах»— всего лишь частный случай, и притом довольно искусственный, общей проблемы классификации иррациональностей. Именно ее будут атаковать с разных сторон в последние десятилетия века, и многочисленные разрозненные результаты будут накапливаться, подготавливая почву для синтетической работы Штейница.

В отношении прежде всего алгебраических иррациональностей фундаментальный принцип классификации доставила теорема Галуа, сводившая изучение алгебраического уравнения к изучению его группы. В самом деле, основным объектом изучения в чистой Алгебре в то время становится теория групп перестановок, о которой нет нужды говорить здесь подробнее (ср. Исторические замечания к гл. I). Другие достижения теории алгебраических полей связаны с развитием в тот же период Теории чисел и Алгебраической геометрии. Эти достижения, впрочем, относятся главным образом к способу изложения и по большей части принадлежат Дедекинду (XVIII), который ввел понятия поля и кольца **), а также (в связи со своими исследованиями

*) Если K не содержит всех корней из единицы, пусть E — поле, полученное присоединением к K всех таких корней. Поле $E \cap N$ является абелевым расширением поля K, откуда (пользуясь теоремой о строении конечных абелевых групп) без труда выводится, что для разрешимости группы поля N над K необходимо и достаточно, чтобы была разрешима группа поля E (N) над E. Учитывая, что корни из единицы выражаются «в радикалах», мы видим, что критерий Галуа не зависит от каких бы то ни было предположений о числовом поле K (и, более общо, остается справедливым для всякого поля характеристики нуль). В действительности Галуа не накладывает на K никаких упрощающих ограничений, а проводит индукцию по порядку радикалов, последовательно присоединяемых к полю K ((XV), стр. 43).

**) Слово «поле» («Körper».— *Прим. перев.*) принадлежит самому Дедекинду; слово «кольцо» было введено Гильбертом (Дедекинд называл кольца «порядками»).

по гиперкомплексным системам) систематически развил линейный аспект теории расширений ((XVIII), т. 3, стр. 33 и далее). Ему также принадлежит мысль рассматривать группу Галуа как состоящую уже из автоморфизмов соответствующего расширения, а не только как группу перестановок корней уравнения. Он доказывает (для числовых полей) фундаментальную теорему о линейной независимости автоморфизмов ((XVIII), т. 3, стр. 29) и устанавливает существование нормального базиса у всякого расширения Галуа ((XVIII), т. 2, стр. 433). Наконец, он приступает к задаче описания алгебраических расширений бесконечной степени, констатирует, что теория Галуа в ее обычном виде здесь неприменима (ибо не всякая подгруппа группы Галуа совпадает с группой расширения относительно какого-нибудь подрасширения) и дерзким взлетом интуиции уже предугадывает необходимость рассматривать группу Галуа как топологическую группу *) — идея, которая достигнет зрелости лишь в 1928 году, когда Крулль разовьет теорию расширений Галуа бесконечной степени (XXIV).

Параллельно с этим развитием уточняется понятие элемента, трансцендентного над полем. Существование трансцендентных чисел впервые устанавливает Лиувилль в 1844 году с помощью явной конструкции, основанной на теории диофантовых приближений (XVIII). В 1874 году Кантор предлагает новое, «неконструктивное» доказательство, использующее простые соображения о мощности множеств (ср. § 3, упражнение 1). Наконец, в 1873 году Эрмит доказывает трансцендентность числа e, а в 1882 году Линдеманн аналогичным методом устанавливает трансцендентность π, положив конец старинной задаче о квадратуре круга **).

Что касается роли трансцендентных чисел в алгебраических выкладках, Кронекер в 1882 году замечает, что если число x трансцендентно над полем K, то поле $K(x)$ изоморфно полю рациональных дробей $K(X)$ ((XIXa), стр. 7). Впрочем, присоединение переменных к полю становится краеугольным камнем его изложения теории алгебраических чисел (XIXa). С другой стороны, Дедекинд и Вебер в том же году ((XVIII), т. 1, стр. 238) показывают, как арифметические методы могут служить для обоснования теории алгебраических кривых. Так в разных направлениях проявляются аналогии между Арифметикой и Алгебраической геометрией, которым суждено оказаться исключительно плодотворными для развития обеих наук.

Во всех этих исследованиях изучаемые поля состоят из «конкретных» элементов в смысле классической математики — чисел (комплексных) или функций от комплексных переменных ***). Но уже Кронекер в 1882 году вполне

---

*) «*Совокупность этих перестановок образует в некотором смысле непрерывное многообразие — вопрос, который мы не будем углублять далее*».

**) Простые доказательства этих теорем можно найти, например, в книге: D. Hilbert, Gesammelte Abhandlungen, Berlin (Springer), 1932, v. I, s. 1.

***) Ни Кронекер, ни Дедекинд и Вебер, как и их предшественники, на самом деле не определяют понятия «алгебраической функции» одной или

отдает себе отчет в том, что (как неясно предчувствовали Гаусс и Галуа) в его теории «переменные» (indeterminées) играют всего лишь роль базисных элементов некоторой алгебры, а не переменных (variables) в смысле Анализа ((XIXa), стр. 93—95). В 1887 году он развивает эту идею в связи с обширной программой, направленной не более и не менее как на преобразование всей математики в целом с отбрасыванием всего, что нельзя свести к алгебраическим операциям над целыми числами (ср. Исторические замечания к Книге I, гл. IV). Именно по этому поводу, следуя идее Коши (XVI), который определил поле C комплексных чисел как поле вычетов $R\ [X]/(X^2+1)$, Кронекер показывает, что теория алгебраических чисел совершенно не зависит от «основной теоремы алгебры» и даже от теории вещественных чисел, ибо всякое поле алгебраических чисел (конечной степени) изоморфно полю вычетов $Q\ [X]/(f)$ (f — неприводимый над Q многочлен) (XIXб). Как замечает Вебер (XX) через несколько лет, развивая первый набросок аксиоматической теории полей, этот метод Кронекера в действительности применим к любому основному полю K. Вебер указывает, в частности, что в качестве K можно взять поле $Z/(p)$ (p — простое число), вводя тем самым в теорию полей исчисление сравнений «по модулю p». Последнее зародилось во второй половине XVIII века в работах Эйлера, Лагранжа, Лежандра и Гаусса, и его аналогия с теорией алгебраических уравнений неоднократно отмечалась. Развивая эту аналогию, Галуа (в своих исследованиях по теории групп), не колеблясь, ввел «идеальные корни» сравнения, неприводимого по модулю p *), и указал их важнейшие свойства ((XV), стр. 15—23) **). Впрочем, применение метода Кронекера к полю $Z/(p)$ приводит (с точностью до терминологии) к представ-

---

нескольких комплексных переменных. В действительности правильно определить «алгебраическую функцию» одной комплексной переменной (в аналитическом смысле) можно, лишь определив предварительно соответствующую риманову поверхность, тогда как именно введение римановой поверхности (чисто алгебраическими средствами) и было целью Дедекинда и Вебера. Этот мнимый порочный круг, разумеется, исчезает, коль скоро поле «алгебраических функций» определяется как абстрактное алгебраическое расширение поля рациональных функций. В действительности, только этим определением и пользуются Дедекинд и Вебер, что вполне узаконивает их результаты.

*) В рукописи, предположительно датируемой 1799 годом, но опубликованной лишь посмертно, Гаусс уже изложил идею введения таких «мнимостей» и получил значительную часть результатов Галуа ((XIII), т. II, стр. 212—240, в особенности стр. 217).

**) Галуа отчетливо сознает формальный характер алгебраических вычислений, не колеблясь, например, брать производную от левой части сравнения, чтобы доказать, что последнее не имеет кратных «мнимых» корней ((XV), стр. 18). Он подчеркивает, в частности, что теорема о примитивном элементе справедлива для конечных полей так же, как и для числовых ((XV), стр. 17, примечание 2), впрочем, не доказывая этого.

лению теории «мнимостей Галуа», уже данному Серре и Дедекиндом ((XVIII), т. 1, стр. 40).

Ко всем этим примерам «абстрактных полей» в самом конце века прибавились поля нового и совершенно иного типа — поля формальных степенных рядов, введенные Веронезе (XXI) и особенно p-адические поля Гензеля (XXII). Именно это последнее открытие привело Штейница (по его собственному свидетельству) к выделению абстрактных понятий, общих всем этим теориям, в фундаментальном труде (XXIII), который можно рассматривать как зарождение современной концепции Алгебры. Систематически развивая следствия из аксиом коммутативного поля, Штейниц вводит понятия кратного поля, сепарабельных (алгебраических) элементов, совершенного поля, определяет степень трансцендентности расширения и, наконец, доказывает существование алгебраически замкнутых расширений любого поля.

В самое последнее время теория Штейница была дополнена в нескольких важных отношениях. С одной стороны, работы Артина с очевидностью выявили линейный характер теории Галуа (XXV). С другой стороны, общее понятие дифференцирования (скопированное с формальных свойств классического дифференциального исчисления), предвосхищенное Дедекиндом ((XVIII), т. 2, стр. 412) и введенное Штейницем в частном случае поля рациональных дробей ((XXIII), стр. 209—212), было с успехом использовано в (важном для современной Алгебраической геометрии) изучении трансцендентных расширений, в частности в обобщении на эти последние понятия сепарабельности (XXVI).

БИБЛИОГРАФИЯ

(I) O. Neugebauer, Vorlesungen über Geschichte der antiken Mathematik, т. I: Vorgriechische Mathematik, Berlin (Springer), 1934. [Русск. перевод: О. Нейгебауэр, Лекции по истории античных математических наук, т. I: Догреческая математика, ОНТИ, М.— Л., 1937.]

(II) Euclidis Elementa, 5 тт., изд. J. L. Heiberg, Lipsiae (Teubner), 1883—1888.

(II bis) T. L. Heath, The thirteen books of Euclid's Elements.., 3 тт., Cambridge, 1908.

(III) H. Cardano, Opera, Lyon, 1663.

(IV) R. Bombelli, L'Algebra, Bologne (G. Rossi), 1572.

(V) Francisci Vietae, Opera mathematica..., Lugduni Batavorum (Elzevir), 1646.

(VI) A. Girard, Invention nouvelle en Algebre, Amsterdam, 1629.

(VII) R. Descartes, Geometria, trad. latine de Fr. van Schooten, 2-е изд., 2 тт., Amsterdam (Elzevir), 1659—1661.

(VIII) G. W. Leibniz, Mathematische Schriften, изд. C. I. Gerhardt, 7 тт., Berlin — Halle (Asher — Schmidt), 1849—1863.

(IX) Der Briefwechsel von Gottfried Wilhelm Leibniz mit Mathematikern, herausg. von C. I. Gerhardt, т. I, Berlin (Mayer und Müller), 1899.

(X) L. Euler, Opera Omnia (1), т. VI, Berlin — Leipzig (Teubner), 1921: а) De Formis Radicum Aequationum..., стр. 1—19; б) De Resolutione Aequationum cujusvis gradus, стр. 170—196.

(XI) J.-L. Lagrange, Œuvres, т. III, Paris (Gauthier-Villars) 1869: а) Reflexiones sur la résolution algébrique des équations, p. 205—421; б) Sur la forme des racines imaginaires des equations, стр. 479.

(XII) A. Vandermonde, Mémoire sur la résolution des équations, Hist. de l'Acad. royale des sciences, année 1771, Paris (1774), стр. 365—416.

(XIII) C. F. Gauss, Werke, I—X, Göttingen, 1863—1923.

(XIV) N. H. Abel, Œuvres, 2 тт., изд. Sylow et Lie, Christiania, 1881.

(XV) E. Galois, Œuvres mathématiques, Paris (Gauthier-Villars), 1897.

(XVI) A.-L. Gauchy, Œuvres completes (1), т. X, Paris (Gauthier-Villars), 1897, стр. 312 и 351.

(XVII) J. Liouville, Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébriques, Journ. de Math. (1), т. XVI (1851), стр. 133.

(XVIII) R. Dedekind, Gesammelte mathematische Werke, 3 тт., Braunschweig (Vieweg), 1932.

(XIX) L. Kronecker: a) Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. de Crelle, т. XCII (1882), стр. 1—122 (-Werke, т. II, Leipzig (Teubner), 1897, стр. 245—387); б) Ein Fundamentalsatz der allgemeinen Arithmetik, J. de Crelle, т. C (1887), стр. 490—510 (-Werke, т. III_I, Leipzig (Teubner), 1899, стр. 211—240).

(XX) H. Weber, Untersuchungen über die allgemeinen Grundlagen der Galois'schen Gleichungstheorie, Math. Ann., т. XLIII (1893), стр. 521—544.

(XXI) G. Veronese, Fondamenti di geometria, Padova, 1891.

(XXII) K. Hensel, Theorie der algebraischen Zahlen, Leipzig — Berlin (Teubner), 1908.

(XXIII) E. Steinitz, Algebraische Theorie der Körpern, J. de Crelle, т. CXXXVII (1910), стр. 167—309.

(XXIV) W. Krull, Galoische Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., т. C (1928), стр. 687.

(XXV) A. Artin, Galois Theory..., Ann. Arbor, 1946.

(XXVI) A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. Coll. Public., т. XXIX, New York, 1946.

ГЛАВА VI

УПОРЯДОЧЕННЫЕ ГРУППЫ И ПОЛЯ

§ 1. Упорядоченные группы. Делимость

Понятия и результаты, изложенные в этом параграфе, касаются изучения отношения порядка в коммутативных моноидах (гл. I, § 1, n° 3), важным примером которых являются *абелевы группы*. Кроме специально оговариваемых случаев, закон композиции в изучаемых группах будет записываться *аддитивно*, как, например, в применениях к теории интегрирования. С другой стороны, попутно мы изложим некоторые важные алгебраические приложения теории упорядоченных моноидов и групп и будем переводить по мере надобности часть результатов на используемый в этих приложениях *мультипликативный* язык.

1. Определение упорядоченных моноидов и групп

Определение 1. *Говорят, что на множестве M структура коммутативного моноида* (в аддитивных обозначениях) *и структура порядка* (обозначаемая знаком $\leqslant$) *согласованы, если они удовлетворяют следующей аксиоме*:

(УМ) *Для любого $z \in M$ отношение $x \leqslant y$ влечет $x + z \leqslant y + z$. Множество M, снабженное согласованными структурами коммутативного моноида и порядка, называется упорядоченным моноидом; если структура коммутативного моноида является структурой абелевой группы, то M называется упорядоченной группой.*

Аналогично можно определить понятие некоммутативного упорядоченного моноида (упражнение 1).

Если структура порядка согласована со структурой моноида, то та же согласованность имеет место и для структуры *противоположного порядка*.

Примеры. 1) Аддитивные группы целых рациональных и всех рациональных чисел являются упорядоченными группами, если они снабжены структурами порядка, определенными в гл. I, § 2, n°5 и § 9, n°5. *То же справедливо и для аддитивной группы действительных чисел (Общ. топол., гл. IV, § 1, n°3).*

2) *Аддитивная группа конечных числовых функций, определенных на множестве E, является упорядоченной группой со структурой порядка, определенной отношением «для любого $x \in E$, $f(x) \leqslant g(x)$», которое записывается «$f \leqslant g$». Это отношение означает, что график функции f лежит под графиком функции g; в некоторых случаях читатель может найти эту графическую интерпретацию удобной.*

Замечание. В главе, посвященной нормированиям, мы увидим, каким образом некоторые структуры упорядоченной группы, используемые в алгебре, допускают такую функциональную интерпретацию.

Согласно общим определениям (Теор., мн. Рез., § 8) взаимно однозначное отображение f упорядоченного моноида M на упорядоченный моноид M' называется *изоморфизмом* M на M', если структура M' получена переносом структуры M с помощью канонических продолжений отображения f. Равносильное требование: f — такое отображение M на M', что $f(x+y) = f(x) + f(y)$ (т. е. представление моноида M на моноид M') и что соотношения $x \leqslant y$ и $f(x) \leqslant f(y)$ эквивалентны (отсюда следует, в частности, что из $f(x) = f(y)$ вытекает $x = y$, т. е. f взаимно однозначно).

Предложение 1 («сложение неравенств»). *Пусть* (x_i) *и* (y_i) $(1 \leqslant i \leqslant n)$ — *две последовательности из* n *элементов, принадлежащих упорядоченному моноиду* M, *такие, что для всякого* i $x_i \leqslant y_i$; тогда

$$x_1 + \ldots + x_n \leqslant y_1 + \ldots + y_n.$$

Если, сверх того, все элементы x_i, y_i *регулярны* (гл. I, § 2, определение 4) (*в частности, если* M — *группа*) *и если существует такое* i, *что* $x_i < y_i$, *то* $x_i + \ldots + x_n < y_1 + \ldots + y_n$.

Случай произвольного n получается индукцией из случая $n = 2$; в индуктивном доказательстве второго утверждения используется тот факт, что сумма регулярных элементов является регулярным элементом (гл. I, § 2, n° 2, предложение 2). Первое

утверждение является следствием соотношений $x_1 + x_2 \leqslant x_1 + y_2$ и $x_1 + y_2 \leqslant y_1 + y_2$, вытекающих из предположений теоремы и определения (УМ). Если даже $x_1 + x_2 = y_1 + y_2$, то $x_1 + x_2 = x_1 + y_2 = y_1 + y_2$, откуда при регулярных x_1 и y_2 $x_2 = y_2$ и $x_1 = y_1$, что доказывает второе утверждение.

Предложение 2. *В упорядоченной группе G неравенства $x \leqslant y$ и $x + z \leqslant y + z$ эквивалентны.*

В самом деле, от одного к другому можно перейти прибавлением к обеим частям z или $(-z)$.

Этот факт означает, что в упорядоченной группе структура порядка *инвариантна относительно сдвигов*. Другими словами, в упорядоченной группе сдвиг является *автоморфизмом* структуры *порядка*.

Следствие. *В упорядоченной группе G отношения $x \leqslant y$, $0 \leqslant y - x$, $x - y \leqslant 0$ и $-y \leqslant -x$ эквивалентны.*

Действительно, достаточно применить предложение 2, беря последовательно $z = -x$, $z = -y$ и $z = -(x + y)$.

Из этого следствия вытекает, в частности, что если G — упорядоченная группа, то отображение $x \to -x$ группы G на себя преобразует структуру порядка в структуру *противоположного порядка*.

2. *Предупорядоченные моноиды и группы*

Если отношение $x \preccurlyeq$ между элементами множества E рефлексивно и транзитивно, но оно называется отношением *предпорядка* на E (Теор. мн., ч. III). Отношение «$x \preccurlyeq y$ и $y \preccurlyeq x$» является отношением эквивалентности S в E (Теор. мн., Рез., § 6, n° 1), согласованным с отношением $x \preccurlyeq y$. Отношение $\preccurlyeq$ определяет на фактормножестве E/S отношение порядка, называемое ассоциированным с $\preccurlyeq$.

Определение 2. *Говорят, что на множестве M отношение предпорядка (обозначаемое $\preccurlyeq$) и структура коммутативного моноида согласованы, если они удовлетворяют следующей аксиоме:*

(ПУМ) *Для любого $z \in M$, $x \preccurlyeq y$ влечет $x + z \preccurlyeq y + z$. Множество M, снабженное структурой коммутативного моноида и согласованным с ней отношением предпорядка, называется предупорядоченным моноидом.*

Пусть M — предупорядоченный моноид и S — отношение эквивалентности «$x \preccurlyeq y$ и $y \preccurlyeq x$». В силу свойства (ПУМ) отношение $x \equiv x' \pmod{S}$ влечет для каждого $y \in M$ отношения $x + y \preccurlyeq x' + y$ и $x' + y \preccurlyeq x + y$, т. е. $x + y \equiv x' + y \pmod{S}$. Другими словами, отношение эквивалентности S *согласовано* со сложением в M (гл. I, § 4, n° 3, определение 4). Тогда M/S с индуцированным законом сложения и структурой порядка, ассоциированной с $\preccurlyeq$, становится *упорядоченным моноидом*. В случае, когда M — предупорядоченная *группа*, M/S является факторгруппой M по подгруппе M', элементы x которой удовлетворяют соотношениям $x \preccurlyeq 0$ и $0 \preccurlyeq x$.

3. *Положительные элементы*

Пусть G — предупорядоченная группа с отношением предпорядка $\preccurlyeq$; из отношений $0 \preccurlyeq x$ и $0 \preccurlyeq y$ вытекают отношения $y \preccurlyeq x + y$ (с помощью свойства (ПУМ)) и $0 \preccurlyeq x + y$ (по транзитивности); это означает, что множество P тех элементов $x \in G$, для которых $0 \preccurlyeq x$, замкнуто относительно сложения; кроме того, отношение $x \preccurlyeq y$ эквивалентно $0 \preccurlyeq y - x$, т. е. тому, что $y - x \in P$.

Обратно:

Предложение 3. *Пусть P — часть абелевой группы G, содержащая 0 и такая, что $P + P \subset P$; тогда отношение $y - x \in P$ есть отношение предпорядка, согласованное со структурой группы G. Для того чтобы это отношение определяло на G структуру упорядоченной группы, необходимо и достаточно, чтобы $P \cap (-P) = \{0\}$; для того чтобы группа G при этой структуре была совершенно упорядоченной группой, необходимо и достаточно, чтобы, кроме того, $P \cup (-P) = G$.*

Непосредственно убеждаемся, что отношение $y - x \in P$ рефлексивно и транзитивно и (если записать его как $x \preccurlyeq y$) удовлетворяет аксиоме (ПУМ). Чтобы доказать второе утверждение, достаточно заметить, что множество $P \cap (-P)$ является такой подгруппой G', что для всех $x \in G'$ $x \preccurlyeq 0$ и $0 \preccurlyeq x$. Наконец, совершенная упорядоченность группы G означает, что для любых элементов x, $y \in G$ один из элементов $x - y$, $y - x$ принадлежит P, чем доказательство заканчивается.

Определение 3. *В упорядоченной группе положительным (соответственно отрицательным) элементом называют всякий элемент x, такой что $0 \leqslant x$ (соответственно $x \leqslant 0$).*

Отметим, что нуль — единственный *одновременно положительный и отрицательный* элемент; всякий элемент x, для которого $0 < x$ (соответственно $x < 0$), называется *строго положительным* (соответственно *строго отрицательным*).

Пример. Пусть в аддитивной группе $Z \times Z$ P — множество элементов (x, y), удовлетворяющих двум неравенствам $ax + by \geqslant 0$, $cx + dy \geqslant 0$, где a, b, c и d — некоторые фиксированные целые числа (*или действительные числа*) такие, что $ad - bc \neq 0$; «конус» P удовлетворяет двум первым условиям предложения 3. Таким образом, на $Z \times Z$ определяются различные структуры порядка, согласованные со структурой группы. При любой из этих структур группа не является совершенно упорядоченной.

Замечание. Используя условие $P + P \subseteq P$, из отношения $x \geqslant 0$ можно вывести отношение $nx \geqslant 0$ для каждого целого натурального n в упорядоченной группе G. Если к тому же положительный элемент x группы G имеет конечный порядок n, то и элемент $-x = (n-1)x$ положителен, так как $P \cap (-P) = \{0\}$, то $x = 0$. В частности, если все элементы группы G имеют конечный порядок, то $P = \{0\}$; отношение $x \leqslant y$ тогда эквивалентно $x = y$ (*дискретная* структура порядка).

4. *Фильтрующиеся группы*

Говорят, что упорядоченное множество G *фильтруется вправо* (соответственно *влево*) (Теор. мн., Рез., § 6), если для каждой пары элементов (x, y) множества G существует такой элемент $z \in G$, что $x \leqslant z$ и $y \leqslant z$ (соответственно $z \leqslant x$, $z \leqslant y$). Каждая упорядоченная группа, фильтрующаяся вправо, фильтруется также влево и обратно: в самом деле, так как существует элемент $z \in G$, для которого $-x \leqslant z$ и $-y \leqslant z$, имеем $-z \leqslant x$ и $-z \leqslant y$ (следствие предложения 2). Поэтому мы будем говорить просто фильтрующаяся группа.

Предложение 4. *Для того чтобы упорядоченная группа G была фильтрующейся, необходимо и достаточно, чтобы она порождалась своими положительными элементами, другими словами, чтобы всякий элемент из G был разностью двух положительных элементов.*

В самом деле, если группа G фильтруется, то для каждого $x \in G$ существует такой положительный элемент z, что $x \leqslant z$, и x есть разность положительных элементов z и $z - x$. Если, обратно, $x = u - v$ и $y = w - t$, где u, v, w, t положительны, то элемент $u + w$ больше x и y.

Предложение 5. *Пусть (x_i) — конечное семейство элементов фильтрующейся группы G; тогда существует такой элемент z, что $x_i + z$ положительны для всех i.*

Пусть $x_i = u_i - v_i$, где u_i и v_i положительны; достаточно взять в качестве z сумму всех v_i.

5. *Отношения делимости в поле*

Мы собираемся определить здесь некоторые упорядоченные группы, играющие важную роль в Алгебре. В этих группах обычно используются мультипликативные обозначения; для того чтобы применить к ним полученные ранее результаты, необходимо, следовательно, перевести все с аддитивного языка на мультипликативный, что не составит никакой трудности для читателя. *Всюду ниже A обозначает область целостности с единицей, записываемой 1* (т. е. ненулевое коммутативное кольцо с единицей и без делителей нуля; см. гл. I, § 8, n° 3); *через K обозначается поле отношений кольца A* (гл. I, § 9, n° 4).

В мультипликативной группе K^* всех ненулевых элементов поля K множество $P = A^*$ ненулевых элементов кольца A замкнуто относительно умножения, поскольку A не имеет делителей нуля. Поэтому множество A^* определяет на K^* отношение предпорядка $x^{-1}y \in P$, т. е. «существует элемент $z \in A^*$, для которого $y = zx$», превращающее K^* в *предупорядоченную группу* (которая записывается мультипликативно) (предложение 3). Распространяя на случай, когда x, $y \in K^*$, терминологию, относящуюся к элементам кольца A (гл. I, § 8, n° 3), отношение $x^{-1}y \in P$ можно прочесть также так: *x делит y*, или *x есть делитель y*, или *y кратно x* (относительно кольца A); мы будем говорить, что отношение $x^{-1}y \in P$ есть *отношение делимости* в K^* относительно кольца A. Отношение «x делит y» мы записываем $x \mid y$, а его отрицание как $x \nmid y$. Элементы из A^* и только они являются *кратными единицы*; они называются иногда *целыми* элементами в K.

Замечания. 1) Отношение делимости в K^* существенно зависит от выбора кольца A. Если $A = K$, то получаем «тривиальное» отношение, где $x \mid y$ для каждой пары (x, y) элементов из K. Пусть p (соответственно q) — простое число; рациональные числа r/s, знаменатель которых делится на p (соответственно q), образуют подкольцо Z_p (соответственно Z_q) кольца Q; отношения делимости в Q^*, соответствующие этим двум кольцам, различны, если $p \neq q$; число p/q кратно 1 для одного кольца, но не для другого.

2) Мы распространяем иногда определение отношения $x \mid y$ на пару элементов из K (а не только из K^*); понимая его как синоним утверждения «существует такой элемент $z \in A$, что $y = zx$»; следовательно, $x \mid 0$ для каждого $x \in K$. Это позволяет сформулировать без ограничений следующий результат: если $x \mid y$ и $x \mid z$, то $x \mid (y - z)$; если $x \mid y$ и $x \nmid z$, то $x \nmid (y - z)$. Расширим таким же образом соответствующую терминологию; в частности, будем говорить, что элемент 0 — целый в K.

Чтобы вывести из отношения делимости отношение *порядка* (n° 2), нужно перейти к факторгруппе группы K^* по подгруппе U элементов $x \in K^*$ таких, что $x \mid 1$ и $1 \mid x$. Эти элементы являются в A^* *делителями* 1, т. е. они обратимы в A; их называют часто для краткости *единицами* кольца A. Факторгруппа K^*/U будет тогда упорядоченной группой. Два элемента x и y из K, принадлежащие одному классу по модулю U, называются *ассоциированными*; это означает, что $x \mid y$ и $y \mid x$. Если, напротив, x делит y, но y не делит x, то говорят, что x строго делит y, или что x есть *строгий делитель* y, или y *строго кратен* x.

Отметим, что K^*/U является *фильтрующейся* группой, поскольку K — поле отношений для A (предложение 4).

Утверждение, что два элемента x и y поля K ассоциированы, в силу транзитивности отношения делимости, означает, что x и y имеют одно и то же множество кратных в K. В соответствии с общими определениями (гл. I, § 1, n° 1) для каждого $x \in K$ символом Ax обозначается множество элементов вида zx, где $z \in A$; множество Ax является подмодулем кольца K, рассматриваемого как A-модуль. Расширяя терминологию, относящуюся к случаю, когда $x \in A$, мы будем называть Ax *главным дробным идеалом* поля K относительно кольца A.

Отметим, что если $A \neq K$, то главный дробный идеал $\neq (0)$ *не является* идеалом в поле K, рассматриваемом как кольцо.

Главный дробный идеал Ax обозначается также через (x). Для противопоставления идеалы кольца A будут называться *целыми*. Мы пишем $x \equiv 0 \pmod{y}$, если $x \in Ay$, и $x \equiv x' \pmod{y}$, если $x - x' \in Ay$; если $x \equiv x' \pmod{y}$, то $zx \equiv zx' \pmod{zy}$, каков бы ни был элемент $z \in K$.

Отметим, что из сравнения $x \equiv x' \pmod{y}$ *не следует* сравнение $zx \equiv zx' \pmod{y}$, по крайней мере если z не целый. Так, в поле Q относительно Z имеем $4 \equiv 2 \pmod{2}$, но не $2 \equiv 1 \pmod{2}$.

Отношение $x \mid y$, очевидно, эквивалентно включению $(x) \supset (y)$. Отображение $x \to (x)$ группы K^* на множество $\mathfrak{P}^*$ ненулевых главных дробных идеалов поля K определяет, следовательно, *взаимно однозначное* отображение факторгруппы K^*/U на $\mathfrak{P}^*$. Перенося на $\mathfrak{P}^*$ посредством этого отображения структуру группы K^*/U, приходим к определению произведения главных дробных идеалов (x) и (y). Этим произведением является идеал (xy), зависящий только от (x) и (y). Наделенное таким законом композиции и отношением порядка $(x) \supset (y)$ множество $\mathfrak{P}^*$ становится упорядоченной группой, изоморфной K^*/U, которую удобно отождествить с K^*/U посредством вышеупомянутого отображения.

Отметим, что отношение «x делит y», которое в случае целых положительных чисел *влечет неравенство* $x \leqslant y$, соответствует включению $(x) \supset (y)$, то есть идеал (x) «больше» идеала (y). Чтобы это «обращение порядка» запомнилось, укажем, например, что 7 имеет «больше» кратных, чем 91.

Отношение $x \mid y$, распространенное на все элементы поля K, также эквивалентно включению $(x) \supset (y)$ в множестве $\mathfrak{P}$ всех главных дробных идеалов поля K (в котором (0) — наименьший элемент относительно включения).

Мы вернемся теперь к аддитивной терминологии как в предшествующих пунктах. Однако после введения аддитивной терминологии в абзацах, отмеченных знаком (ДЕЛ), будут введены соответствующие термины, связанные с делимостью. (В этих абзацах мы сохраняем обозначения этого пункта.)

Для облегчения работы читателя на язык Делимости будут переведены также некоторые важные результаты. Перевод предложения 7, например, будет обозначаться так: «Предложение 7 (ДЕЛ)».

6. *Элементарные операции над упорядоченными группами*

Пусть H — *подгруппа* упорядоченной группы G; ясно, что структура порядка, индуцированная на H структурой порядка группы G, согласована с групповой структурой на H. Всегда будет предполагаться, что подгруппа H снабжена этой структурой порядка, за исключением тех случаев, когда будет оговорено противное. Если P — множество положительных элементов группы G, то множеством положительных элементов подгруппы H служит $H \cap P$.

Пусть (G_α) — семейство упорядоченных групп; согласно определению произведения упорядоченных множеств (Теор. мн., гл. III) произведение групп $G = \prod_\alpha G_\alpha$ снабжено структурой порядка, в которой отношение «$(x_\alpha) \leqslant (y_\alpha)$» между двумя элементами из G по определению есть синоним выражения «$x_\alpha \leqslant y_\alpha$ для любого α». Непосредственно видно, что эта структура порядка согласована с групповой структурой в G. Наделенная этой структурой группа G становится упорядоченной группой, которая называется *произведением упорядоченных групп* G_α. Положительные элементы в G — это те элементы, все компоненты которых положительны. В случае, когда все множители G_α совпадают с одной и той же упорядоченной группой H, G является группой H^I отображений множества индексов I в H, причем отношение «$f \leqslant g$» между двумя отображениями множества I в H означает, что «$f(\alpha) \leqslant g(\alpha)$ для любого $\alpha \in I$»; положительные отображения — это те, которые принимают только положительные значения. *Прямую сумму* семейства (G_α) упорядоченных групп определим как подгруппу их произведения (гл. II, § 1, n° 7).

Пусть $(G_\iota)_{\iota \in I}$ — семейство упорядоченных групп, в котором множество индексов I *вполне упорядочено* отношением порядка $\leqslant$; напомним (Теор. мн., гл. III), что на множестве произведения $G = \prod_\iota G_\iota$ оно определяет отношение порядка, называемое «лексикографическим», при котором отношение «$(x_\iota) < (y_\iota)$» между двумя элементами из G по определению является синонимом выражения «если β — наименьший из таких индексов ι, что $x_\iota \neq y_\iota$, то $x_\beta < y_\beta$». Напомним, что произведение вполне упоря-

доченного семейства *совершенно упорядоченных* множеств само совершенно упорядочено посредством лексикографического порядка. В общем случае отношение лексикографического порядка на G согласовано со структурой группы (это проверяется непосредственно); наделенная этой структурой группа G является упорядоченной группой, которая называется *лексикографическим произведением* вполне упорядоченного семейства упорядоченных групп (G_ι).

Замечания. 1) В случае, встречающемся наиболее часто, вполне упорядоченным множеством индексов служит *конечный* интервал $[1, n]$ множества N.

2) Множество положительных элементов лексикографического произведения G состоит из 0 и элементов, у которых ненулевая компонента с наименьшим индексом положительна.

7. *Возрастающие представления упорядоченных групп*

Пусть G и G' — две упорядоченные группы; среди представлений f структуры аддитивной группы G в структуру аддитивной группы G' можно рассматривать возрастающие отображения, то есть такие, для которых из $x \leqslant y$ следует, что $f(x) \leqslant f(y)$. В силу соотношения $f(y - x) = f(y) - f(x)$ возрастающие представления группы G в группу G' характеризуются тем, что при таком представлении образ положительного элемента из G является положительным элементом в G'. Пусть P (соответственно P') — множество положительных элементов в G (соответственно в G'); условие возрастания записывается так:

$$f(P) \subset P'.$$

Ясно, что каноническое отображение любой подгруппы группы G в упорядоченную группу G' и проекция произведения упорядоченных групп на его множители являются возрастающими представлениями.

Изоморфизм (n° 1) f упорядоченной группы G на упорядоченную группу G' — это взаимно однозначное представление группы G на G' такое, что f и представление, обратное к нему, являются возрастающими. Это записывается так:

$$f(P) = P'.$$

Может случиться, что изоморфизм групповой структуры группы G на групповую структуру группы G' является возрастающим, в то время как обратный изоморфизм не является таковым. Так будет, например, если $G = G'$, f — тождественное отображение группы G на себя и если $P \subset P'$, но $P \neq P'$. В частности, в Z в качестве P' можно взять множество (обычных) целых положительных чисел, а в качестве P — множество четных положительных чисел.

(ДЕЛ) Пусть K — поле $F_2(X)$ рациональных дробей над полем F_2 из двух элементов. Отношения делимости относительно колец $F_2[X] = A'$ и $F_2[X^2, X^3] = A$ определяют на K^* две различные структуры упорядоченной группы такие, что $A \subset A'$ (это структуры упорядоченной группы, поскольку 1 является единственной единицей как в A, так и в A').

8. *Верхняя и нижняя грани в упорядоченной группе*

Напомним (Теор. мн., Рез., § 6, n° 7), что если множество мажорант части A упорядоченного множества E (иными словами, множество таких элементов $z \in E$, что $x \leqslant z$ для всех $x \in A$) допускает наименьший элемент a, то этот элемент (являющийся тогда единственным) называется *верхней гранью* части A. Если A — множество элементов некоторого семейства $(x_\iota)_{\iota \in I}$ элементов из E, его верхняя грань, если она существует, обозначается символом $\sup_{\iota \in I} x_\iota$ (или $\sup_\iota x_\iota$, или просто $\sup x_\iota$). Если речь идет о конечном семействе (x_i) $(1 \leqslant i \leqslant n)$, эта грань обозначается также символом $\sup(x_1, \ldots, x_n)$. Нижняя грань определяется аналогичным образом и обозначается inf. Операции sup и inf *ассоциативны* и *коммутативны*.

Напомним (Теор. мн., гл. III), что если F — часть упорядоченного множества E, а (x_ι) — семейство элементов из F, то из существования верхней грани $\sup(x_\iota)$ в E (которую можно обозначать через $\sup_E(x_\iota)$) не следует существование верхней грани семейства x_ι в F (которую, если она существует, можно обозначить через $\sup_F(x_\iota)$. Если каждая из них существует, то $\sup_E(x_\iota) \leqslant \sup_F(x_\iota)$; однако если $\sup_E(x_\iota)$ существует и принадлежит F, то верхняя грань $\sup_F(x_\iota)$ существует и равна $\sup_E(x_\iota)$. Например, в кольце многочленов $A = K[X, Y]$ над полем K главные идеалы AX и AY относительно включения имеют верхней гранью идеал $AX + AY$ во множестве всех идеалов и кольцо A во множестве главных идеалов кольца A.

(ДЕЛ) Элемент d группы K^* называется *наибольшим общим делителем* или, короче, н. о. д. семейства (x_ι) элементов из K^*, если главный дробный идеал (d) является в $\mathfrak{F}^*$ *верхней гранью* (относительно включения) семейства идеалов $((x_\iota))$ или, иначе говоря, если для элемента $z \in K^*$ отношение $z \mid d$ эквивалентно тому, что «$z \mid x_\iota$ для каждого ι». Аналогично, элемент $m \in K^*$ называется *наименьшим общим кратным*, или н. о. к. семейства (x_ι), если предел (m) является *нижней гранью* семейства идеалов $((x_\iota))$ в $\mathfrak{F}^*$, то есть если соотношение $m \mid z$ эквивалентно тому, что «$x_\iota \mid z$ для каждого ι». Н. о. д. и н. о. к., если они существуют, определены по модулю подгруппы U единиц K^*, то есть всякие два н. о. д. (или два н. о. к.) данного семейства ассоциированы; для краткости часто обозначают через н. о. д. (x_ι) и н. о. к. (x_ι) любой н. о. д. из н. о. д. или н. о. к. семейства (x_ι), если такие элементы существуют.

(ДЕЛ) Иногда понятие н. о. д. распространяют и на семейства (x_ι) таких элементов из K, некоторые из которых могут быть равны нулю; в этом случае н. о. д. определяется как такой элемент d из K, что $z \mid d$ эквивалентно выражению «$z \mid x_\iota$ для любого ι».

Очевидно, $d = 0$, если каждый из x_ι равен нулю; в остальных случаях d совпадает с н. о. д. ненулевых элементов данного семейства. Аналогично, н. о. к. семейства, некоторые элементы которого равны нулю, есть нуль.

В упорядоченной группе G из инвариантности порядка относительно сдвигов (предложение 2) немедленно следует равенство

$$\sup(z + x_\iota) = z + \sup(x_\iota) \tag{1}$$

в том смысле, что каждый раз, когда одна из частей этого равенства существует, то другая. также существует и равна первой. Точно так же, поскольку отображение $x \to -x$ преобразует порядок группы G в противоположный (согласно предложению 2), получаем

$$\inf(-x_\iota) = -\sup(x_\iota) \tag{2}$$

— соотношение, имеющее тот же смысл, что и предыдущее.

Предложение 6. *Пусть* $(x_\alpha)_{\alpha \in A}$, $(y_\beta)_{\beta \in B}$ — *два семейства элементов упорядоченной группы* G, *каждое из которых обладает верхней гранью. Тогда семейство* $(x_\alpha + y_\beta)_{(\alpha,\beta) \in A \times B}$ *также имеет*

верхнюю грань, и

$$\sup_{(\alpha,\beta)\in A\times B}(x_\alpha + y_\beta) = \sup_{\alpha\in A} x_\alpha + \sup_{\beta\in B} y_\beta.$$

Действительно, из неравенств $x_\alpha + y_\beta \leqslant z$ для любого α и любого β следует, что $\sup(x_\alpha) + y_\beta \leqslant z$ для любого β, а отсюда $\sup(x_\alpha) + \sup(y_\beta) \leqslant z$.

9. *Решеточно-упорядоченные группы*

Напомним, что упорядоченное множество, в котором каждая конечная *непустая* часть обладает верхней и нижней гранями, называется *решеткой* (Теор. мн., Рез., § 6, n° 8). Ясно, что произведение решеточно-упорядоченных групп, в частности, произведение совершенно упорядоченных групп, является решеточно-упорядоченной группой. В противоположность этому подгруппа решеточно-упорядоченной группы не обязана быть решеточно-упорядоченной группой.

Так, в упорядоченной группе $Z \times Z$ «вторая биссектриса» (множество пар (n, n') таких, что $n + n' = 0$) упорядочена дискретно и, следовательно, не является решеточно-упорядоченной группой.

Аддитивная группа многочленов от одной действительной переменной (упражнение 2, n° 1) является фильтрующейся группой (поскольку $p(x)$ и $q(x)$ мажорируются многочленом $(p(x))^2 + (q(x))^2 + 1$), которая, можно показать, не является решеточно-упорядоченной группой.

В оставшейся части этого параграфа упорядоченные моноиды группы, если не оговорено противное, будут предполагаться *решеточно-упорядоченными*.

Читатель заметит, что предложения 7, 10 и 11 справедливы в любой упорядоченной группе в том смысле, что если одна из верхних или нижних граней, фигурирующих в формулировке этих предложений, существуют, то существует и другая, и высказанные соотношения имеют место.

Предложение 7. *Пусть x и y — элементы решеточно-упорядоченной группы G; тогда* $x + y = \inf(x, y) + \sup(x, y)$.

Действительно, согласно соотношениям (1) и (2), (n° 8),

$$\sup(a - x, a - y) = a + \sup(-x, -y) = a - \inf(x, y);$$

достаточно взять $a = x + y$.

Предложение 7 (ДЕЛ). *Если $\mathscr{P}^*$ — решеточно-упорядоченная группа, то для любой пары элементов a и b из K произведение наибольшего общего делителя и наименьшего общего кратного элементов a и b ассоциировано с их произведением ab.*

Предложение 8. *Пусть P — множество положительных элементов упорядоченной группы G. Для того чтобы G была решеточно-упорядочена, необходимо и достаточно, чтобы $G = P - P$ и, кроме того, чтобы множество P, наделенное индуцированным порядком, удовлетворяло одному из следующих условий:*

а) *каждая пара элементов из P имеет в P верхнюю грань.*

б) *каждая пара элементов из P имеет в P нижнюю грань.*

Необходимость этих условий очевидна: действительно, соотношения $G = P - P$ означают, что G фильтруется (предложение 4); с другой стороны, поскольку нижняя и верхняя грани *в* G двух элементов из P положительны, то они также лежат в P.

Обратно, заметим сначала, что в предложении а) (соответственно б)) каждая пара элементов x, y из P имеет верхнюю (соответственно нижнюю) грань *в* G, равную своей верхней грани a (соответственно своей нижней грани b) *в* P. Это очевидно для a, поскольку каждая мажоранта элементов x и y положительна.

Пусть теперь $z \in G$ — миноранта для x и y; тогда существует такой элемент $u \in P$, что $z + u \in P$, поскольку $G = P - P$; однако элемент $\inf_P(x+u,\ y+u)$ мажорирует $b+u$ и, значит, имеет вид $b+c+u\ (c \geqslant 0)$; так как $b+c$ меньше, чем x и y, то $c = 0$; значит, $\inf_P(x+u,\ y+u) = b+u$, откуда $z+u \leqslant b+u$, так что $z \leqslant b$ и, следовательно, b является нижней гранью для x и y в G. Пусть теперь x и y — произвольные элементы из G; мы сдвинем их в P: пусть элемент $v \in P$ таков, что $x+v$ и $y+v$ положительны (предложение 5); по предположению а) (соответственно b)) $x+v$ и $y+v$ допускают верхнюю (соответственно нижнюю) грань в P, а значит, и в G, что мы только что проверили. Обратный сдвиг показывает, что x и y допускают верхнюю (соответственно нижнюю) грань в G; существование одного из двух родов граней для каждой пары $(x,\ y)$ влечет существование другого в силу соотношения (2) (n° 8), это доказывает достаточность условий теоремы.

10. Теорема о разложении

Теорема 1 (теорема о разложении). *Пусть* $(x_i)_{1\leqslant i\leqslant p}$ *и* $(y_j)_{1\leqslant j\leqslant q}$ *— две конечные последовательности положительных элементов решеточно-упорядоченной группы* G *такие, что* $\sum_{i=1}^{p} x_i = \sum_{j=1}^{q} y_j$; *тогда существует двойная последовательность* $(z_{ij})_{1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q}$ *положительных элементов из* G *такая, что* $x_i = \sum_{j=1}^{q} z_{ij}$ *для каждого* i *и* $y_j = \sum_{i=1}^{p} z_{ij}$ *для каждого* j.

1° Докажем сначала теорему при $p=q=2$. Пусть x, x', y, y' — такие положительные элементы из G, что $x+x'=y+y'$. Положим $a=\sup(0,\ x-y')$. Так как элемент $x-y'=y-x'$ меньше чем x и y, элементы $b=x-a$ и $c=y-a$ положительны; то же верно и для $d=a-(x-y')$. Имеем $x=a+b$, $x'=c+d$, $y=a+c$, $y'=b+d$.

2° Покажем теперь, что если теорема справедлива для $p<m$ и $q=n$ $(m>2,\ n\geqslant 2)$, то она верна и для $p=m$, $q=n$. Согласно предположению имеем $x_m+\sum_{i=1}^{m-1} x_i = \sum_{j=1}^{n} y_j$. Поскольку теорема верна при $p=2$, $q=n$, существуют две такие конечные последовательности (z'_j), (z''_j) из n положительных членов, что $\sum_{i=1}^{m-1} x_i = \sum_{j=1}^{n} z'_j$, $x_m = \sum_{j=1}^{n} z''_j$ и $y_j = z'_j + z''_j$ для $1\leqslant j\leqslant n$. С другой стороны, поскольку теорема справедлива для $p=m-1$ и $q=n$, существует двойная последовательность $(u_{ij})_{1\leqslant i\leqslant m-1,\ 1\leqslant j\leqslant n}$ такая, что $x_i = \sum_{j=1}^{n} u_{ij}$ для $1\leqslant i\leqslant m-1$ и $z'_j = \sum_{i=1}^{m-1} u_{ij}$ для $1\leqslant j\leqslant n$. Полагая $z_{ij}=u_{ij}$ при $1\leqslant i\leqslant m-1$ и $z_{mj}=z''_j$ $(1\leqslant j\leqslant n)$, получаем двойную последовательность, удовлетворяющую условиям теоремы.

3° Меняя роли элементов x_i и y_i, видим точно так же, что если теорема верна для $p=m$ и $q<n$ $(m\geqslant z,\ n>2)$, то она справедлива для $p=m$, $q=n$. Таким образом, теорема доказывается двойной индукцией, отправляясь от случая $p=2$, $q=2$.

Следствие. *Пусть* y, x_1, x_2, ..., x_n — *набор* $n+1$ *таких положительных элементов группы* G, *что* $y \leqslant \sum_{i=1}^{n} x_i$; *тогда существуют* n *положительных элементов* y_i $(1 \leqslant i \leqslant n)$ *таких, что* $y_i \leqslant x_i$ *и* $y = \sum_{i=1}^{n} y_i$.

Достаточно применить теорему 1 к последовательности x_i и последовательности, состоящей из двух элементов y и $z = (\sum_{i=1}^{n} x_i) - y$.

11. Положительная и отрицательная части

Определение 4. *В решеточно-упорядоченной группе* G *положительной частью* (*соответственно отрицательной частью, абсолютным значением*) *элемента* $x \in G$ *называется и обозначается через* x^+ (*соответственно* x^-, $|x|$) *элемент* $\sup(x, 0)$ (*соответственно* $\sup(-x, 0)$, $\sup(x, -x)$).

Несмотря на свое название, отрицательная часть x^- элемента x является *положительным* элементом.

Ясно, что $x^- = (-x)^+$ и $|-x| = |x|$. Отметим также следующие формулы, первая из которых есть непосредственное следствие определений и инвариантности порядка относительно сдвигов, а вторая выводится из первой при помощи предложения 7:

$$\sup(x, y) = x + (y-x)^+, \quad \inf(x, y) = y - (y-x)^+. \tag{3}$$

Предложение 9. а) *Для каждого элемента* x *решеточно-упорядоченной группы* G *имеют место соотношения:* $x = x^+ - x^-$ *и* $\inf(x^+, x^-) = 0$.

б) *Для каждого представления элемента* x *в виде разности двух положительных элементов* $x = u - v$ *имеют место равенства:* $u = x^+ + w$, $v = x^- + w$, *где* $w = \inf(u, v)$. *Если, в частности,* $\inf(u, v) = 0$, *то* $u = x^+$, $v = x^-$.

в) *отношение* «$x \leqslant y$» *эквивалентно* «$x^+ \leqslant y^+$ *и* $x^- \geqslant y^-$»

г) $|x| = x^+ + x^- \geqslant 0$.

д) *Каковы бы ни были элементы x и y из G, справедливо неравенство* $|x+y|\leqslant|x|+|y|$ *и более общее неравенство* $|\sum_{i=1}^{n} x_i|\leqslant\sum_{i=1}^{n}|x_i|$ *для любого конечного семейства (x_i) элементов группы G.*

е) *Каковы бы ни были элементы x и y из G, справедливо неравенство* $|\,|x|-|y|\,|\leqslant|x-y|$.

Мы докажем одновременно а) и б). Если $x=u-v$, где u и v положительны, то $u\geqslant x$, значит, $u\geqslant\sup(x,\ 0)=x^+$, и элемент $w=u-x^+$ положителен. С другой стороны,

$$x^+-x=\sup(x,\ 0)-x=\sup(x-x,\ -x)=x^-,$$

откуда следует, что $x=x^+-x^-$ и $v-x^-=w$. Из $z\leqslant x^-$ вытекает, что $z\leqslant x^+-x$ и $x\leqslant x^+-z$; если, кроме того, $z\leqslant x^+$, то элемент x^+-z положителен, откуда $x^+\leqslant x^+-z$ в силу определения x^+. Итак, $z\leqslant 0$, поэтому $\inf(x^+,\ x^-)=0$, откуда, применяя сдвиг, $\inf(u,\ v)=w$.

в) Из соотношения $x\leqslant y$ следует, что $\sup(y,\ 0)\geqslant x$ и $\sup(y,\ 0)\geqslant 0$, откуда $x^+\leqslant y^+$; из $-y\leqslant -x$ выводим точно так же $x^-\geqslant y^-$. Обратная импликация тотчас же получается из равенств $x=x^+-x^-$ и $y=y^+-y^-$.

г) Так как $x\leqslant x^+$ и $-x\leqslant x^-$, ясно, что

$$|x|=\sup(x,\ -x)\leqslant x^++x^-.$$

Обратно, из неравенств $a\geqslant x$ и $a\geqslant -x$ в силу в) следует, что $a^+\geqslant x^+$, $a^+\geqslant x^-$, $a^-\leqslant x^-$, $a^-\leqslant x^+$. Так как элемент a^- положителен и $\inf(x^+,\ x^-)=0$, два последних неравенства показывают, что $a^-=0$ и $a=a^+$; два первых дают тогда $a\geqslant\sup(x^+,\ x^-)$, т. е. a больше элемента, равного x^++x^-, в силу а) и предложения 7.

д) Из неравенств $x\leqslant|x|$ и $y\leqslant|y|$ получаем $x+y\leqslant|x|+|y|$; из неравенств $-x\leqslant|x|$ и $-y\leqslant|y|$ вытекает, что $-x-y\leqslant|x|+|y|$, откуда следует первое неравенство. Второе выводится индукцией по n.

е) Заменяя в д) x и y на y и $x-y$, приходим к неравенству

$$|x|-|y|\leqslant|x-y|;$$

точно так же $|y|-|x|\leqslant|y-x|=|x-y|$, откуда получаем сформулированный результат.

Замечание. Из в) следует, что соотношение $|x|=0$ влечет $x=0$ (ибо x^+ и x^- положительны); следовательно, неравенство $x\neq 0$ означает, что $|x|>0$.

Предложение 9 (ДЕЛ). *Если группа $\mathfrak{P}^*$ главных дробных идеалов в K решеточно-упорядочена, то каждый элемент x из K^* можно представить в виде $x=uv^{-1}$, где u и v — некоторые целые такие, что н. о. д. $(u, v)=1$. Для любого другого представления $x=u'v'^{-1}$ элемента x в виде частного двух целых имеют место соотношения $u'=uw$, $v'=vw$, где w — целый элемент, равный н. о. д. элементов u' и v'; в частности, если н. о. д. $(u', v')=1$, то u' и v' ассоциированы соответственно с u и v.*

Такое представление uv^{-1} элемента x из K^* часто называется *несократимой дробью*.

12. Независимые элементы

Определение 5. *Элементы x и y решеточно-упорядоченной группы называются независимыми, если* $\inf(x, y)=0$.

В некоторых случаях независимыми следует называть два таких элемента x и y, для которых $\inf(|x|, |y|)=0$ (см. Интегр., ч. II, § 1) или ввести соответствующую терминологию в теорию Делимости. Мы этого здесь не будем делать.

Два независимых элемента обязательно *положительны*. Положительная и отрицательная части элемента x, т. е. элементы x^+ и x^- независимы (предложение 9а)). Говорят, что элементы x_ι семейства $(x_\iota)_{\iota\in I}$ *независимы в совокупности*, если $\inf\limits_{\iota\in I}(x_\iota)=0$; для этого достаточно, чтобы существовала такая конечная часть J множества I, что соответствующие элементы независимы в совокупности. Элементы семейства (x_ι) называются *попарно независимыми*, если $\inf(x_\iota, x_\varkappa)=0$ для каждой пары $(\iota, \varkappa)$ различных индексов.

Элементы x_ι могут быть независимы в совокупности, но не быть попарно независимыми.

Если x и y независимы, то говорят также, что x не зависит от y, или что y не зависит от x.

(ДЕЛ) Элементы x и y в K называются *независимыми*, если главные идеалы (x) и (y) независимы в $\mathfrak{P}$. Это означает, что

единица является н. о. д. элементов x и y, откуда следует, что x и y — *целые*.

Например, числитель и знаменатель несократимой дроби независимы. Понятия попарно независимых целых элементов и целых элементов, независимых в совокупности, определяются аналогично.

(ДЕЛ) Независимые элементы x и y часто называют «взаимно простыми»; условимся избегать этой терминологии, которая приводит к путанице с понятием целого простого элемента (гл. VII, § 1, n° 3).

Предложение 10. *Пусть x, y, z — три элемента решеточно-упорядоченной группы; для того чтобы $x-z$ и $y-z$ были независимы, необходимо и достаточно, чтобы $z=\inf(x, y)$.*

Действительно, соотношения $z=\inf(x, y)$ и $0=\inf(x-z, y-z)$ эквивалентны.

Предложение 10 (ДЕЛ). *Предположим, что множество $\mathfrak{P}^*$ решеточно-упорядочено, и пусть a, b, c — тройка элементов из K, причем $c\neq 0$; для того чтобы ac^{-1} и bc^{-1} были независимы, необходимо и достаточно, чтобы элемент c был наибольшим общим делителем элементов a и b.*

Предложение 11. *Если x и y — независимые элементы в решеточно-упорядоченной группе и $z\geqslant 0$, то* $\inf(x, z)=\inf(x, y+z)$.

Действительно, $0=\inf(x, y)$, так что $z=\inf(x+z, y+z)$. Следовательно, отношение «$t\leqslant x$ и $t\leqslant z$» совпадает с отношением «$t\leqslant x$ и $t\leqslant x+z$», а значит, также (поскольку $x\leqslant x+z$) с отношением «$t\leqslant x$ и $t\leqslant y+z$».

Следствие 1. *Если x и y независимы и $x\leqslant y+z$ $(z\geqslant 0)$, то $x\leqslant z$.*

Следствие 2. *Если x не зависит от y и z, то x не зависит также и от $y+z$.*

Следствие 3. *Пусть x_i и (y_j) — такие два конечных семейства элементов решеточно-упорядоченной группы G, что ни один x_i не зависит ни от одного из y_i. Тогда $x_1+\ldots+x_n$ не зависит от $y_1+\ldots+y_m$.*

Это выводится из следствия 2 индукцией по m и n.

Следствие 4. *Каково бы ни было целое $n\geqslant 0$, справедливы равенства $(nx)^+=nx^+$ и $(nx)^-=nx^-$; для каждого $n\in Z$, кроме того, $|nx|=|n|\cdot|x|$.*

Действительно, $nx = nx^+ - nx^-$, так как элементы x^+ и x^- независимы, то независимы также nx^+ и nx^- при всех $n \geqslant 0$ (следствие 3); первое утверждение следует отсюда в силу предложения 9а). Второе следует в силу предложения 9а) в случае $n \geqslant 0$; случай $n < 0$ вытекает отсюда с помощью соотношения $|-x| = |x|$.

Предложение 11 (ДЕЛ). *Предположим, что множество $\mathfrak{F}^*$ решеточно-упорядочено, и пусть a, b, c — тройка таких целых элементов в K, что a не зависит от b; тогда всякий н. о. д. элементов a и c является также и н. о. д. для a и bc.*

Следствие 1 (ДЕЛ) («лемма Евклида»). *Пусть a, b, c — три целых элемента из K. Если a не зависит от b и делит bc, то a делит c.*

Следствие 2 (ДЕЛ). *Если x не зависит от y и z, то x не зависит от yz.*

Следствие 3 (ДЕЛ). *Пусть (x_i) и (y_j) — два конечных семейства целых элементов из K такие, что каждый элемент x_i не зависит от каждого y_j. Тогда произведение элементов x_i не зависит от произведения элементов y_j.*

Следствие 4 (ДЕЛ). *Если d — н. о. д. элементов x и y, то d^n — н. о. д. элементов x^n и y^n для всякого целого n.*

В самом деле, xd^{-1} и yd^{-1} — независимые элементы (предложение 10 (ДЕЛ)) и то же самое верно для $x^n d^{-n}$ и $y^n d^{-n}$ (следствие 3).

Предложение 12. *Пусть x_i $(1 \leqslant i \leqslant n)$ — n попарно независимых элементов решеточно-упорядоченной группы. Тогда*

$$\sup(x_1, \ldots, x_n) = x_1 + \ldots + x_n.$$

Так как элемент x_i независим от $x_1 + \ldots + x_{i-1}$ при всех $2 \leqslant i \leqslant n$ (следствие 3 предложения 11), это равенство выводится из формулы $u + v = \sup(u, v) + \inf(u, v)$ (предложение 7) индукцией по n.

Замечание. Предложение 7 показывает также, что для того, чтобы x и y были независимы, необходимо и достаточно, чтобы $x + y = \sup(x, y)$.

Предложение 12 (ДЕЛ). *Пусть a_i суть n попарно независимых целых элементов из K. Тогда их произведение $a_1 \ldots a_n$ является н. о. к. элементов $a_1, \ldots, a_n$.*

Предложение 13. *Пусть в решеточно-упорядоченной группе G дано множество (x_α), допускающее нижнюю (соответственно верхнюю) грань y и произвольный элемент $z \in G$; тогда множество $(\sup(z, x_\alpha))$ (соответственно $(\inf(z, x_\alpha))$) обладает нижней (соответственно верхней) гранью, причем имеем соответственно*

$$\left.\begin{aligned} \inf_\alpha (\sup(z, x_\alpha)) &= \sup(z, \inf_\alpha x_\alpha), \\ \sup_\alpha (\inf(z, x_\alpha)) &= \inf(z, \sup_\alpha x_\alpha). \end{aligned}\right\} \tag{4}$$

В самом деле, $\sup(z, x_\alpha) = z + (x_\alpha - z)^+$, поэтому при помощи сдвига мы можем свести все к случаю $z = 0$. Другими словами, достаточно показать, что множество (x_α^+) обладает нижней гранью, равной y^+. Так как $y \leqslant x_\alpha$, то $y^+ \leqslant x_\alpha^+$ для каждого α (предложение 9в)). Если, обратно, $a \leqslant x_\alpha^+$ для каждого α, то $a \leqslant x_\alpha + x_\alpha^-$ (предложение 9а)); но из $y \leqslant x_\alpha$ следует, что $y^- \geqslant x_\alpha^-$; поэтому $a \leqslant x_\alpha + y^-$ для каждого α; другими словами, $a \leqslant y + y^- = y^+$. Вторая формула выводится аналогично с заменой sup на inf.

Следствие. *Если элемент z решеточно-упорядоченной группы G не зависит от каждого из элементов x_α, образующих семейство с верхней гранью y, то z не зависит от y.*

Это непосредственно вытекает из второй формулы (4).

Замечание. Применяя формулы предложения 13 к множеству из двух элементов x, y, получим следующие формулы, выражающие, что в решеточно-упорядоченной группе каждая из двух операций sup и inf *дистрибутивна* относительно другой:

$$\sup(z, \inf(x, y)) = \inf(\sup(z, x), \sup(x, y)),$$
$$\inf(z, \sup(x, y)) = \sup(\inf(z, x), \inf(z, y)).$$

Это свойство дистрибутивности является специальным свойством решеточно-упорядоченных групп; оно не распространяется ни на множества, ни даже на решеточно-упорядоченные моноиды (см. упражнение 24).

13. *Экстремальные элементы*

Определение 6. *Элемент x упорядоченной группы G называется экстремальным, если он является минимальным в множестве строго положительных элементов группы G.*

Пусть x — экстремальный элемент упорядоченной группы G. Для всякого положительного элемента $y \in G$ элемент $\inf(x, y)$,

если он существует, может быть равен только либо x, либо 0. Таким образом, в решеточно-упорядоченной группе каждый положительный элемент либо больше, либо независим с экстремальным элементом x; в частности, разные экстремальные элементы независимы.

(ДЕЛ) Целый элемент p в K называется *экстремальным*, если идеал (p) является экстремальным элементом упорядоченной группы $\mathcal{F}^*$. Это означает, что каждый целый элемент, делящий p, ассоциирован либо с p, либо с 1. Если группа $\mathcal{F}^*$ решеточно-упорядочена, то всякий целый элемент a либо независим с p, либо кратен p.

Замечание. 1) Тот факт, что целый элемент p является экстремальным, *не означает*, что (p) — максимальный идеал кольца A (см. упражнение 26). 2) В некоторых случаях употребляют вместо слова экстремальный слово *простой* (например, для целых рациональных чисел см. гл. VII, § 1, n° 4) или слово *неприводимый* для полиномов (см. гл. VII, § 1, n° 5).

Предложение 14. *Для того чтобы элемент $x>0$ структурно-упорядоченной группы был экстремальным, необходимо и достаточно, чтобы из отношений «$x\leqslant y+z$, $0\leqslant y$, $0\leqslant z$» следовало отношение «$x\leqslant y$ или $x\leqslant z$».*

Если x экстремален, то, как мы только что видели, y либо больше x, либо не зависит от x; в последнем случае следствие 1 из предложения 11 показывает, что z больше x. Обратно, предположим, что условие теоремы выполнено: из $0\leqslant y\leqslant x$ выводим, полагая $x=y+z$ $(z\geqslant 0)$, что либо $x\leqslant y$, либо $x\leqslant z$. В первом случае $x=y$, во втором $x\leqslant x-y$, следовательно, $y\leqslant 0$, а значит, $y=0$; это показывает, что x действительно экстремальный.

Отметим, что мы не пользовались решеточной упорядоченностью группы G при доказательстве достаточности условия.

Предложение 14 (ДЕЛ). *Пусть $\mathcal{F}^*$ — решеточно-упорядоченная группа. Необходимое и достаточное условие экстремальности целого элемента $p\in K$ заключается в том, что p должен быть отличен от единицы, и если p делит произведение двух целых элементов, то p делит хотя бы один из них.*

Предложение 15. *Пусть G' — подгруппа решеточно-упорядоченной группы G, порожденная множеством $(p_\iota)_{\iota\in I}$ попарно различных экстремальных элементов группы G. Каждый элемент*

$x \in G'$ можно однозначно представить в виде $x = \sum_\iota n_\iota p_\iota$, где n_ι — целые рациональные числа, отличные от нуля только для конечного числа индексов. Для того чтобы элемент x был положительным, необходимо и достаточно, чтобы все n_ι были положительными.

Ясно, что G' — множество элементов из G, представленных в виде $\sum n_\iota p_\iota$. Предположим, что $\sum_\iota n_\iota p_\iota \geqslant 0$. Перенося в правую часть все члены с коэффициентами $n_\iota < 0$, получаем соотношение вида

$$m_1 p_1 + \ldots + m_r p_r \geqslant n_1 q_1 + \ldots + n_s q_s,$$

где $r \geqslant 0$, $s \geqslant 0$ и p_i, q_j составляют множество из $r+s$ различных экстремальных элементов; следствие 3 предложения 11 показывает тогда, что правая и левая части неравенства независимы, и следовательно, $s = 0$. Отсюда видно, что из соотношения $\sum_\iota n_\iota p_\iota \geqslant 0$ следует положительность n_ι для всех ι. Поэтому из равенства $\sum n_\iota p_\iota = 0$ вытекает одновременно, что $n_\iota \geqslant 0$ и $n_\iota \leqslant 0$ для всех ι, т. е. $n_\iota = 0$, и это завершает доказательство.

Этот результат означает, что упорядоченная группа G' изоморфна группе $Z^{(I)}$ — прямой сумме упорядоченных групп Z (n° 6). Упорядоченные группы $Z^{(I)}$ можно охарактеризовать следующим способом:

Теорема 2. *Для того чтобы упорядоченная группа G была изоморфна прямой сумме групп Z (упорядоченных обычным образом) необходимо и достаточно, чтобы она была решеточно-упорядочена и удовлетворяла следующему условию:*

(МИН) *Каждое непустое множество положительных элементов группы G, наделенное отношением порядка, индуцированным отношением порядка в группе G, содержит минимальный элемент.*

Покажем сначала, что группа $Z^{(I)}$ решеточно-упорядочена и удовлетворяет условию (МИН). Она является решеточно-упорядоченной группой, поскольку это прямая сумма совершенно упорядоченных групп. С другой стороны, пусть E — непустое множество положительных элементов из $Z^{(I)}$; пусть $x = \sum_\iota n_\iota e_\iota$ — любой элемент множества E [(e_ι) — канонический базис группы $Z^{(I)}$]. Число положительных элементов $y \in Z^{(I)}$, которые меньше x, конеч-

но и равно $\prod_\iota (n_\iota + 1)$ (лишь конечное число множителей в этом произведении отлично от единицы). Следовательно, множество F элементов из E, меньших x, и подавно конечно; так как оно непусто, оно содержит минимальный элемент y (Теор. мн., гл. III), который является, очевидно, минимальным элементом в E.

Предположим наоборот, что условие (МИН) удовлетворено. Сначала докажем следующую лемму:

Лемма. *Пусть G — упорядоченная группа, удовлетворяющая условию* (МИН). *Для каждого элемента $x > 0$ из G существует экстремальный элемент $p \in G$ такой, что $p \leqslant x$.*

В самом деле, множество положительных элементов группы G, меньших x, непусто и обладает минимальным элементом p, который, очевидно, будет экстремальным в группе G.

Приняв это во внимание, вернемся к доказательству теоремы 2. Чтобы применить предложение 15, нам достаточно показать, что группа G порождается своими экстремальными элементами. Так как G — фильтрующаяся группа, то достаточно показать (предложение 4), что каждый элемент $x > 0$ в группе G является суммой экстремальных элементов. Для этого рассмотрим множество E тех положительных элементов $y \in G$, которые представимы в форме $y = x - (p_1 + \ldots + p_n)$, где p_i — экстремальные элементы группы G, не обязательно различные. Так как $x > 0$, то в силу леммы множество E не пусто. Следовательно, E содержит некоторый минимальный элемент q в силу свойства (МИН). В случае $q \neq 0$, элемент q в силу леммы был бы больше некоторого экстремального элемента p' группы G и элемент $q - p'$ принадлежал бы E, что противоречит минимальности q в E. Следовательно, $q = 0$ и $x = p_1 + \ldots + p_n$, что и требовалось доказать.

Теорема 2 найдет в дальнейшем применение в теории Делимости в кольцах главных идеалов (гл. VII, § 1, n° 2) и в кольцах частных (Вторая часть, глава, относящаяся к нормированиям) и в изучении идеалов дедекиндовых колец (там же).

Упражнения. 1) Упорядоченный некоммутативный моноид M есть моноид (записываемый мультипликативно), снабженный такой структурой порядка, что отношение $x \leqslant y$ влечет $zx \leqslant zy$ и $xz \leqslant yz$ для каждого $z \in M$. Пусть G — упорядоченная некоммутативная группа. Доказать следующие утверждения:

а) Пусть P — множество элементов, больших чем нейтральный элемент $e \in G$, тогда $P \cdot P = P$, $P \cap P^{-1} = \{e\}$, и $aPa^{-1} = P$ для

каждого $a \in G$. Обратить утверждение. Найти условие для совершенной упорядоченности группы G.

б) Если один из элементов $\sup(x, y)$, $\inf(x, y)$ существует, то другой также существует и $\sup(x, y) = x\,(\inf(x, y))^{-1} = y\,(\inf(x, y))^{-1}\,x$.

в) Элементы $\sup(x, e)$ и $\sup(x^{-1}, e)$ перестановочны. Два независимых элемента перестановочны.

г) Подгруппа G', порожденная экстремальными элементами группы G, коммутативна. Отсюда следует, что если выполнены условия теоремы 2, то G — коммутативная группа.

2) Пусть E — решетка, на которой задан закон композиции $(x, y) \to xy$ (не обязательно ассоциативный) такой, что для каждого $a \in E$ отображения $x \to ax$ и $x \to xa$ являются изоморфизмами упорядоченного множества E на себя. Обозначим через x_a (соответственно a^x) элемент из E, определенный равенством $(x_a)\,a = x$ (соответственно $a\,({}_a x) = x$), и предположим, что отображения $x \to a_x$ и $x \to {}_x a$ являются изоморфизмами упорядочекного множества E на множество E, снабженное противоположным порядком. Показать, что при этих условиях для любых x, y, z имеет место равенство

$$(z_{\inf(x, y)})\,x = (z_y)\,(\sup x,\ y).$$

3) Пусть G — упорядоченная группа, множество P положительных элементов которой не сводится к нулю. Показать, что G бесконечна и не может обладать ни наибольшим, ни наименьшим элементами.

4) Пусть G — упорядоченная группа, P — множество положительных элементов группы G, f — каноническое отображение группы G на *факторгруппу* G/H. Для того чтобы множество $f(P)$ определяло на G/H структуру упорядоченной группы, необходимо и достаточно, чтобы из условий $0 \leqslant y \leqslant x$ и $x \in H$ следовало, что $y \in H$. Тогда H называется *изолированной* подгруппой группы G, и G/H рассматривается как упорядоченная группа. Если G к тому же решеточно-упорядочена, то для того, чтобы G/H была группой-решеткой, необходимо и достаточно, чтобы из соотношений $|y| < |x|$ и $x \in H$ вытекало, что $y \in H$. Показать, что этот факт равносилен тому, что H — изолированная и фильтрующаяся подгруппа. Показать, что упорядоченная группа G, не имеющая других изолированных подгрупп, кроме себя и $\{0\}$, является совершенно упорядоченной (рассмотреть изолированные подгруппы, порожденные двумя положительными элементами из G); *вывести отсюда (Общ. топол., гл. V, § 3, упражнение 1), что G изоморфна тогда подгруппе аддитивной группы действительных чисел.

5) Дать пример упорядоченной группы с недискретным отношением порядка, обладающей ненулевыми элементами конечного порядка (взять факторгруппу подходящей упорядоченной группы G по такой подгруппе H, что $P \cap H = \{0\}$).

6) Пусть G — упорядоченная группа, P — множество ее положительных элементов. Показать, что $P - P$ является наибольшей

фильтрующейся подгруппой группы G и что это изолированная подгруппа. Каково отношение порядка в факторгруппе?

7) Если в группе Z в качестве множества положительных элементов взять множество, состоящее из нуля и целых чисел $\geqslant 2$, то полученная упорядоченная группа будет фильтрующейся, но не решеточно-упорядоченной. (Показать, что множество тех x, для которых $x \geqslant 0$ и $x \geqslant 1$, обладает двумя разными минимальными элементами.)

8) Пусть x — такой элемент упорядоченной группы, что существует $y = \inf(x, 0)$; тогда для любого целого числа $n > 0$ из $nx \geqslant 0$ вытекает, что $x \geqslant 0$ (имеем $ny = \inf(nx, (n-1)x, \ldots, 0) \geqslant \geqslant \inf((n-1)x, \ldots, 0) = (n-1)y$); следовательно, равенство $nx = 0$ влечет $x = 0$.

9) Показать, что в решеточно-упорядоченной группе сумма всякого семейства (H_α) изолированных и фильтрующихся подгрупп является изолированной и фильтрующейся подгруппой. (Использовать следствие теоремы 1.)

10) Показать, что в решеточно-упорядоченной группе G для каждой конечной последовательности элементов (x_i) $(1 \leqslant i \leqslant n)$ из G справедливо соотношение

$$\sup(x_i) = \sum_i x_i - \sum_{i<j} \inf(x_i, x_j) + \ldots + (-1)^{p+1} \times$$
$$\times \sum_{i_1<i_2<\ldots<i_p} \inf(x_{i_1}, \ldots, x_{i_p}) + \ldots + (-1)^{n+1} \inf(x_1, \ldots, x_n).$$

(Рассуждать по индукции, отправляясь от предложения 7 и используя дистрибутивность операции sup относительно операции inf.)

11) Пусть (x_i) — семейство из n элементов в решеточно-упорядоченной группе G; для каждого целого k $(1 \leqslant k \leqslant n)$ через d_k (соответственно m_k) обозначим нижнюю (соответственно верхнюю) грань сумм k различных элементов x_i; число таких сумм равно $\binom{n}{k}$. Показать, что

$$d_k + m_{n-k} = x_1 + x_2 + \ldots + x_n.$$

12) Подгруппа H решеточно-упорядоченной группы G называется *корешеточно-упорядоченной*, если для каждой пары элементов $x, y \in H$, также $\sup_G(x, y) \in H$ (эта верхняя грань, следовательно, совпадает с $\sup_H(x, y)$).

а) Если $G = Q \times Q \times Q$ (группа Q упорядочена обычным образом), то подгруппа H тех элементов (x, y, z), для которых $z = x + y$ решеточно-упорядочена, но не корешеточно упорядочена.

б) Каждая изолированная (упражнение 4) фильтрующаяся подгруппа решеточно-упорядоченной группы является корешеточно-упорядоченной.

в) Пусть G — решеточно-упорядоченная группа, H — некоторая подгруппа в G, H' — множество нижних граней конечных частей из H и H'' — множество верхних граней конечных частей из H'. Показать, что H'' — наименьшая корешеточно-упорядоченная подгруппа, содержащая H (используя замечание к предложению 3).

13) Говорят, что моноид M *полурешеточно-упорядочен снизу* (или, для краткости, *полурешеточно-упорядочен*), если M — упорядоченный моноид, $\inf(x, y)$ существует для любой пары x, y элементов из M и если $\inf(x+z, y+z)=\inf(x, y)+z$ для любых x, y, $z\in M$. Доказать, что тогда справедливы тождества

$$\inf(x, z)+\inf(y, z)=\inf(x+y, z+\inf(x, y, z)),$$

$$\inf(x, y, z)+\inf(x+y, y+z, z+x)=\inf(x, y)+\inf(y, z)+\inf(z, x).$$

С помощью первого тождества доказать, что из неравенств $x\leqslant z$ и $y\leqslant z$ следует, что $x+y\leqslant z+\inf(x, y)$.

Показать, что предложение 11 и его следствие имеют место в полурешеточно-упорядоченных моноидах, обладающих нейтральным элементом.

14) Показать, что в полурешеточно-упорядоченных моноидах имеет место неравенство

$$\inf(x_i+y_i)\geqslant\inf(x_i)+\inf(y_i)$$

для любых конечных последовательностей (x_i) и (y_i), состоящих каждая из n элементов.

Вывести из этого, что в решеточно-упорядоченной группе выполняются неравенства

$$(x+y)^+\leqslant x^++y^+; \qquad |x^+-y^+|\leqslant|x-y|.$$

15) Показать, что в решеточно-упорядоченной группе справедливо тождество

$$|x^+-y^+|+|x^--y^-|=|x-y|.$$

(Заметить, что $x-y\leqslant|x-y|$ и $|x|-|y|<|x-y|$.)

16) Показать, что в полурешеточно-упорядоченном моноиде выполняется соотношение

$$n\inf(x, y)+\inf(nx, ny)=2n\inf(x, y)$$ (сравни упражнение 8).

Доказать, что $\inf(nx, ny)=n\inf(x, y)$, если $\inf(x, y)$ — регулярный элемент.

17) Пусть M — полурешеточно-упорядоченный моноид, обладающий нейтральным элементом нуль, и x, y, z, $t\in M$ таковы, что $z\geqslant 0$, $t\geqslant 0$. Доказать неравенство

$$\inf(x+z, y+t)+\inf(x, y)\geqslant\inf(x+z, y)+\inf(x, y+t).$$

18) Пусть $(G_\iota)_{\iota\in I}$ — семейство совершенно упорядоченных групп с совершенно упорядоченным множеством индексов I; на группе G', являющейся *прямой суммой* групп G_ι, определим структуру упорядоченной группы, беря в качестве положительных элементов группы

G' множество таких (x_ι), что $x_\iota > 0$ для наименьшего индекса ι с ненулевым x_ι. Показать, что группа G', снабженная этой структурой, является совершенно упорядоченной группой.

19) Пусть G — аддитивная группа, (P_α) — семейство частей в G таких, что $P_\alpha + P_\alpha \subset P_\alpha$ и $P_\alpha \cap (-P_\alpha) = \{0\}$; пусть G_α — упорядоченная группа, получающаяся, если в качестве положительных элементов взято множество P_α. Положим $P = \bigcap_\alpha P_\alpha$. Показать, что $P + P \subset P$ и $P \cap (-P) = \{0\}$. Показать, что упорядоченная группа H, получающаяся наделением группы G отношением порядка с множеством P положительных элементов, изоморфна диагонали произведения групп G_α.

20) Пусть G — аддитивная группа, P — часть в G, удовлетворяющая условиям: $1°\ P + P = P$, $2°\ P \cap (-P) = \{0\}$, $3°$ для каждого целого n из включения $nx \in P$ следует, что $x \in P$ (условие C)).

а) Показать, что для элемента $a \in G$ такого, что $a \overline{\in} P$, существует часть P' в G, удовлетворяющая условию (C) в) и такая, что $P \subset P'$ и $-a \in P'$ (в качестве P' взять множество тех $x \in G$, для которых существуют два целых числа $m > 0$ и $n \geqslant 0$ и элемент $y \in P$, удовлетворяющие равенству $mx = -na + y$).

б) Вывести из а), что P является пересечением тех частей $T \subset G$, для которых выполняются равенства; $T + T = T$, $T \cap (-T) = \{0\}$, $T \cup (-T) = G$ (иными словами, тех частей, которые определяют на G структуру совершенно упорядоченной группы) и которые содержат P. (Использовать теорему Цорна.)

в) В частности, если G — аддитивная группа, в которой все ненулевые элементы имеют бесконечный порядок, то пересечение всех таких частей T, для которых $T + T = T$, $T \cap (-T) = \{0\}$ и $T \cup (-T) = G$, сводится к 0.

*21) Упорядоченная группа называется *решеточно-упорядочиваемой*, если она изоморфна подгруппе решеточно-упорядоченной группы. Показать, что для решеточной упорядочиваемости группы G необходимо и достаточно, чтобы для каждого целого $n > 0$ из неравенства $nx \geqslant 0$ следовало бы, что $x \geqslant 0$ (для доказательства достаточности использовать упражнение 20б) и 19). Показать, что каждая решеточно-упорядочиваемая группа изоморфна подгруппе произведения совершенно упорядоченных групп.

22) Пусть G — решеточно-упорядочиваемая группа (рассматриваемая как Z-модуль) и E — векторное пространство $G_{(Q)}$ (гл. III, § 2); показать, что на аддитивной группе E можно однозначно определить структуру порядка, согласованную с групповой структурой на E и индуцирующую на G данную структуру порядка. Пространство E, наделенное этой структурой, является решеточно-упорядочиваемой группой.

23) Пусть G — решеточно-упорядоченная группа $Z \times Z$ (Z наделена обычной структурой порядка) и H — изолированная подгруппа в G,

порожденная элементом (2, —3); показать, что упорядоченная группа G/H не является решеточно-упорядоченной (см. упражнение 4).

24) Пусть A — коммутативное кольцо, а I — множество всех его *идеалов*; *произведением* $\mathfrak{ab}$ двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ назовем идеал, образованный конечными суммами $\sum_i a_i b_i$, где $a_i \in \mathfrak{a}$ и $b_i \in \mathfrak{b}$. Показать, что $\mathfrak{a}(\mathfrak{b}+\mathfrak{f}) = \mathfrak{ab}+\mathfrak{af}$; иначе говоря, множество I, наделенное отношением порядка $\mathfrak{a} \supset \mathfrak{b}$ и законом композиции $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{ab}$, является *полурешеточно-упорядоченным моноидом* (упражнение 13), причем верхней гранью элементов $\mathfrak{a}$ и $\mathfrak{b}$ является идеал $\mathfrak{a}+\mathfrak{b}$, а нижней гранью — $\mathfrak{a} \cap \mathfrak{b}$.

Пусть K — некоторое поле, $A = K[X, Y]$ — кольцо многочленов от двух переменных над K. В кольце A рассмотрим главные идеалы $\mathfrak{a} = (X)$, $\mathfrak{b} = (Y)$ и $\mathfrak{f} = (X+Y)$; показать, что

$$(\mathfrak{a} \cap \mathfrak{b})+\mathfrak{f} \neq (\mathfrak{a}+\mathfrak{f}) \cap (\mathfrak{b}+\mathfrak{f}), \quad (\mathfrak{a}+\mathfrak{b}) \cap \mathfrak{f} \neq (\mathfrak{a} \cap \mathfrak{f})+(\mathfrak{b} \cap \mathfrak{f}),$$
$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a}+\mathfrak{b}) \neq (\mathfrak{a}(\mathfrak{a}+\mathfrak{b})) \cap (\mathfrak{b}(\mathfrak{a}+\mathfrak{b})).$$

*25) Пусть I — полурешеточно-упорядоченный моноид идеалов коммутативного кольца A (упражнение 24). Для того чтобы конечная система сравнений $x \equiv a_i (\mathfrak{a}_i)$ имела решение каждый раз, когда любые два из этих сравнений имеют общее решение (т. е. если $a_i \equiv a_j (\mathfrak{a}_i + \mathfrak{a}_j)$ для каждой пары индексов i, j), необходимо и достаточно, чтобы в I каждая из двух операций $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a} \cap \mathfrak{b}$ и $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a}+\mathfrak{b}$ была дистрибутивна относительно другой («китайская теорема»). Доказательство можно провести следующим образом:

а) Если $(\mathfrak{a}_1 \cap \mathfrak{a}_2)+(\mathfrak{a}_1 \cap \mathfrak{a}_3) = \mathfrak{a}_1 \cap (\mathfrak{a}_2+\mathfrak{a}_3)$ и если каждые два из трех сравнений $x \equiv a_i (\mathfrak{a}_i)$ $(i = 1, 2, 3)$ имеют общее решение, тогда все три сравнения имеют общее решение (пусть x_{12} — общее решение сравнений $x \equiv a_1 (\mathfrak{a}_1)$ и $x \equiv a_2 (\mathfrak{a}_2)$, x_{13} — общее решение сравнений $x \equiv a_1 (\mathfrak{a}_1)$ и $x = a_3 (\mathfrak{a}_3)$; показать, что сравнения $x = x_{12} (\mathfrak{a}_1 \cap \mathfrak{a}_2)$ и $x = x_{13} (\mathfrak{a}_1 \cap \mathfrak{a}_3)$ имеют общее решение).

б) Если каждая система трех сравнений, любые два из которых имеют общее решение, сама обладает общим решением, то выполняются законы дистрибутивности:

$$\mathfrak{a}+(\mathfrak{b} \cap \mathfrak{f}) = (\mathfrak{a}+\mathfrak{b}) \cap (\mathfrak{a}+\mathfrak{f}) \quad \text{и} \quad \mathfrak{a} \cap (\mathfrak{b}+\mathfrak{f}) = (\mathfrak{a} \cap \mathfrak{b})+(\mathfrak{a} \cap \mathfrak{f}).$$

(Для доказательства первого равенства заметить, что для каждого элемента $x \in (\mathfrak{a}+\mathfrak{b}) \cap (\mathfrak{a}+\mathfrak{f})$ существует такой y, что $y \in \mathfrak{b} \cap \mathfrak{f}$, $y \equiv x (\mathfrak{a})$. Для доказательства второго соотношения заметить, что для каждого элемента $x \in \mathfrak{a} \cap (\mathfrak{b}+\mathfrak{f})$ существует такой элемент $y \in \mathfrak{a} \cap \mathfrak{b}$, что $y \equiv x (\mathfrak{f})$.) Отметим, что в силу а) и б) вторая формула дистрибутивности влечет первую.

в) Доказать «китайскую теорему» индукцией по числу рассматриваемых сравнений методом, аналогичным методу доказательства предложения а).

26) Показать, что в моноиде идеалов кольца многочленов $K[X, Y]$ (где K — поле) идеал (X) удовлетворяет условию предложения 14, но не является максимальным.

27) Пусть A — кольцо, являющееся квадратичным расширением кольца Z с базисом $(1, e)$, где $e^2 = -5$.

Показать, что A является областью целостности; в этом кольце $9 = 3 \cdot 3 = (2+e)(2-e)$; показать, что 3, $2+e$, $2-e$ являются экстремальными элементами кольца A, не удовлетворяющими условию предложения 14 (ДЕЛ).

* 28) Пусть G — решеточно-упорядоченная группа, P — множество ее положительных элементов. Два элемента x, $y \in P$ называются *эквивалентными*, если каждый элемент, независимый с первым, не зависит и от второго; классы эквивалентности, соответствующие этому отношению, называются *нитями* в P; через $\bar{x}$ обозначим нить, содержащую x.

а) Пусть $\bar{a}$ и $\bar{b}$ — две нити; пусть x, x_1 — два элемента из $\bar{a}$ и y, y_1 — два элемента из $\bar{b}$; показать, что если каждый элемент, не зависящий от x, не зависит от y, то каждый элемент, не зависящий от x_1, не зависит от y_1. Таким образом определяется отношение между $\bar{a}$ и $\bar{b}$, которое обозначается $\bar{a} \geqslant \bar{b}$; показать, что оно является отношением порядка на множестве F нитей.

б) Показать, что при так определенном отношении порядка F является решеткой и что

$$\inf(\bar{a}, \bar{b}) = \overline{\inf(a, b)}, \quad \sup(\bar{a}, \bar{b}) = \overline{\sup(a, b)} = a + b.$$

(Использовать следствие 2 предложения 11.) Показать, что наименьшим элементом в F является нить $\bar{0} = \{0\}$.

в) Две нити $\bar{a}$ и $\bar{b}$ называются независимыми, если $\inf(\bar{a}, \bar{b}) = \bar{0}$. Показать, что если $\bar{a}$ и $\bar{b}$ — две нити $\neq \bar{0}$ и если $\bar{a} < \bar{b}$, то существует нить $\bar{c} \neq \bar{0}$, независимая с $\bar{a}$ и такая, что $\bar{c} < \bar{b}$.

г) Нить $\bar{m} \neq \bar{0}$ называется экстремальной, если она является минимальным элементом множества отличных от $\bar{0}$ нитей. Показать, что экстремальная нить совершенно упорядочена (пусть a и b — два элемента из $\bar{m}$; рассмотреть нити, которым принадлежат элементы $a - \inf(a, b)$ и $b - \inf(a, b)$ и использовать б)). Показать, кроме того, что объединение нитей $\bar{m}$, $-\bar{m}$ и $\{0\}$ является совершенно упорядоченной подгруппой $H(\bar{m})$ в G.

д) Пусть дано семейство $(\bar{m}_\iota)$ экстремальных нитей в G; показать, что подгруппа H, порождаемая объединением нитей $\bar{m}_\iota$, изоморфна прямой сумме (n° 6) групп $H(\bar{m}_\iota)$ (свести к случаю конечного семейства, а затем провести индукцию).

е) Показать, что в произведении (соответственно в прямой сумме) совершенно упорядоченных групп элементами экстремальных нитей являются в точности те, у которых все координаты, кроме одной (которая >0), равны нулю. Отсюда следует, что упорядоченная группа может быть только одним способом представлена в виде произведения (соответственно прямой суммы) совершенно упорядоченных групп (иначе говоря, множители определены однозначно).

29) Упорядоченная группа G называется *вполне решеточно-упорядоченной*, если она решеточно-упорядочена и если каждая мажорируемая часть в G допускает в G верхнюю грань.

а) Показать, что для полной решеточной упорядоченности фильтрующейся группы G необходимо и достаточно, чтобы каждая часть из множества положительных элементов P группы G имела верхнюю грань в P.

б) Произведение вполне решеточно-упорядоченных групп есть вполне решеточно-упорядоченная группа.

в) Каждая изолированная подгруппа вполне решеточно-упорядоченной группы вполне решеточно-упорядочена.

30) В упорядоченной группе G для каждой части A в G обозначим символом $m(A)$ (соответственно $M(A)$) множество миноранг (соответственно мажорант) части A в G; тогда $m(A)=-M(-A)$.

а) Отношение $A\subset B$ влечет $m(B)\subset m(A)$ и $M(m(A))\subset M(m(B))$.

б) Имеют место включения $A\subset M(m(A))$ и $M(m(M(A)))=M(A)$.

в) Пусть A_ι — семейство частей из G; тогда

$$m(\bigcup_\iota A_\iota)=\bigcap_\iota m(A_\iota).$$

г) Каждое множество $M(B)$, где B — мажорируемая непустая часть в G, называется *высшим множеством* в G. Для каждой минорируемой непустой части A в множество $GM(m(A))$ является наименьшим высшим множеством, содержащим A; его обозначают через $\langle A\rangle$, если $A\subset B$, то $\langle A\rangle\subset\langle B\rangle$; если A имеет верхнюю грань a в G, то $\langle A\rangle=M(a)$; последнее множество обозначает также $\langle a\rangle$.

д) Если A и B — две непустые минорируемые части в G, то $\langle A+B\rangle=\langle\langle A\rangle+\langle B\rangle\rangle$. Отсюда следует, что в множестве $\mathfrak{M}(G)$ высших множеств из G отображение $(A, B)\to\langle A+B\rangle$ является ассоциативным и коммутативным законом композиции, для которого $\langle 0\rangle=P$ — нейтральный элемент, причем отношение порядка $A\supset B$ согласовано с этим законом композиции. Множество $\mathfrak{M}(G)$, наделенное этой структурой, является полурешеточно-упорядоченным моноидом, если G — фильтрующаяся группа. Кроме того, отображение $x\to\langle x\rangle$ группы G в $\mathfrak{M}(G)$ является изоморфизмом упорядоченной группы G на некоторую подгруппу моноида $\mathfrak{M}(G)$.

е) Если элемент A из моноида $\mathfrak{M}(G)$ симметризуем относительно закона композиции в этом моноиде, то симметричным к нему служит

$M(-A) = -m(A)$. (Заметить, что если B симметричен с A, то $B \subset M(-A)$ и $A+M(-A) \subset \langle 0 \rangle$, откуда $\langle A+B \rangle = \langle A+M(-A) \rangle$.)

*31) Упорядоченная группа G называется *архимедовой*, если единственными элементами $x \in G$, для которых множество кратных nx (n — целые > 0) является минорируемым, будут положительные элементы в G.

а) Для того чтобы моноид $\mathfrak{M}(G)$ высших множеств упорядоченной группы G был группой, необходимо и достаточно, чтобы группа G была архимедовой (использовать упражнение 30г)); $\mathfrak{M}(G)$ тогда вполне решеточно-упорядочена.

б) Вывести отсюда, что для того, чтобы упорядоченная группа G была изоморфна подгруппе вполне решеточно-упорядоченной группы, необходимо и достаточно, чтобы G была архимедовой.

*32) а) Пусть G — вполне решеточно-упорядоченная группа и H — подгруппа в G. Для каждого высшего множества A *в группе* H через x_A обозначим нижнюю грань A *в* G. Показать, что отображение $A \to x_A$ множества $\mathfrak{M}(H)$ в группу G взаимно однозначно. (Установить, что A — множество тех элементов $y \in H$, для которых $y \geqslant x_A$.)

б) Обозначим через $\langle B \rangle$, где B — минорируемая часть в H, высшее множество, порожденное частью B в H (элемент множества $\mathfrak{M}(H)$). Пусть для каждой части B в H, минорируемой в H, справедливо соотношение $\inf B = \inf \langle B \rangle$ (нижние грани берутся в G); показать, что в этом случае отображение $A \to x_A$ является изоморфизмом вполне решеточно-упорядоченной группы $\mathfrak{M}(H)$ на некоторую подгруппу группы G (см. упражнение 30д)).

в) Пусть каждый элемент группы G является нижней гранью некоторой части в H; показать, что в этом случае для каждой минорирующей в H части $B \subset H$ выполняется равенство $\inf B = \inf \langle B \rangle$ (нижние грани берутся в G). (Заметить, что это равенство справедливо при условии $\inf B \in H$; в общем случае рассмотреть такой элемент $x \in G$, что $x + \inf B \in H$, т. е. являющийся нижней гранью некоторой части в H, а дальше использовать упражнение 30д).)

г) Пусть G — вполне решеточно-упорядоченная группа $Z \times Z \times R$, $\theta > 0$ — иррациональное число, и пусть H — подгруппа, состоящая из таких элементов (x, y, z), что $\theta(z-x)+y=0$. Показать, что не существует никакого изоморфизма вполне решеточно-упорядоченной группы $\mathfrak{M}(H)$ на подгруппу группы G, сводящегося к тождественному отображению на H. (Показать, что группа $\mathfrak{M}(H)$ изоморфна $K = Z \times R$; рассмотреть в K подгруппу, состоящую из тех u, для которых для каждого целого $n > 0$ существует элемент $v \in E$ с $nv = u$, и аналогичную подгруппу в G.)

33) а) Для того чтобы совершенно упорядоченная группа была архимедовой, необходимо и достаточно, чтобы для каждой пары

элементов $x>0$, $y>0$, принадлежащих G, существовало целое $n>0$ такое, что $y\leqslant nx$.

б) Всякая совершенно упорядоченная и вполне решеточно-упорядоченная группа G изоморфна либо $\{0\}$, либо Z, либо R (отбросив два первых случая, возьмем $a>0$ в G и поставим в соответствие каждому элементу $x\in G$ нижнюю грань тех рациональных чисел p/q, для которых $qx\leqslant pa$).

в) Вывести отсюда, что каждая совершенно упорядоченная архимедова группа изоморфна подгруппе группы R. (Заметить, что множество $\mathfrak{M}(G)$ совершенно упорядочено.)

г) Лексикографическое произведение $Z\times Z$ не является архимедовой группой.

34) Пусть $G=Z^N$ — произведение несчетного семейства совершенно упорядоченных групп Z, $H=Z^{(N)}$ — изолированная и фильтрующаяся подгруппа в G — прямая сумма множителей группы G. Показать, что решеточно-упорядоченная группа G/H (упражнение 4) не может быть архимедовой, хотя G и H вполне решеточно-упорядочены. (Доказать, что для *всякого* элемента $z\in G/H$ последовательность nz (n — целые >0) является минорируемой в G/H.)

*35) Высшее множество A в упорядоченной группе G называется множеством *конечного типа*, если существует такое конечное множество F, что $A=\langle F\rangle$. Группа G называется *полуархимедовой*, если каждое высшее множество конечного типа симметризуемо в моноиде $\mathfrak{M}(G)$. Каждая решеточно-упорядоченная (соответственно архимедова) группа является полуархимедовой (упражнение 31а)).

а) Показать, что каждая полуархимедова группа решеточно-упорядочиваема. (Если $nx\geqslant 0$, рассмотреть высшее множество $\langle F\rangle$, где $F=\{0, x, \ldots, (n-1)x\}$, и показать, что оно симметризуемо.)

°б) Пусть K — лексикографическое произведение $R\times R$, G — обычное произведение $K\times R$. Пусть θ — иррациональное число $0<\theta<1$, H — подгруппа в G, порожденная элементами $((1, 0), 0)$, $((\theta, 0), \theta)$ и $((0, x), 0)$, где x пробегает R. Показать, что подгруппа H произведения двух совершенно упорядоченных групп не является архимедовой. (Рассмотреть высшее множество, порожденное элементами $((1, 0), 0)$ и $((\theta, 0), \theta)$ из H, и показать, что оно не может быть симметризуемым.)

в) Пусть G — фильтрующаяся полуархимедова группа, $\mathfrak{M}_f(G)$ — устойчивое подмножество в $\mathfrak{M}(G)$, порожденное высшими множествами конечного типа и симметричными к ним; показать, что $\mathfrak{M}_f(G)$ — *решеточно-упорядоченная* группа. (Использовать, что множество $\mathfrak{M}(G)$ полурешеточно упорядочено.)

г)° Пусть G — группа $Z\times Z$, в которой в качестве множества P положительных элементов берется множество тех пар (x, y), для которых $x\geqslant 0$, $y\geqslant \theta x$, где θ — некоторое иррациональное число. Показать, что G — архимедова группа, но что симметричное множе-

ство в $\mathfrak{M}(G)$ к высшему множеству конечного типа, не имеющему вида $\langle a\rangle$, не является множеством конечного типа.

36) Пусть G — упорядоченная группа и P — множество ее положительных элементов. Для того чтобы группа G была изоморфна прямой сумме групп Z, необходимо и достаточно, чтобы существовало такое отображение $x \to d(x)$ множества P в N, что если не имеет места неравенство $b \geqslant a$, то в высшем множестве $\langle a, b\rangle$ существует такой элемент c, что $d(c) < d(a)$. (Показать, что это справедливо для $Z^{(I)}$, если положить $d(x) = \sum x_\iota$; обратно, показать, что каждое высшее множество A имеет вид $\langle a\rangle$, для чего рассмотреть такой элемент $a \in A$, что $d(a) \leqslant d(x)$ для каждого $x \in A$, затем применить результат теоремы 2.)

37) Для того чтобы фильтрующаяся группа G была изоморфна подгруппе прямой суммы $Z^{(I)}$, необходимо и достаточно, чтобы: 1° G была архимедова; 2° каждое высшее множество в G являлось множеством конечного типа. (Показать, что условие 2° эквивалентно условию (МИН) (теор. 2) в упорядоченном моноиде $\mathfrak{M}(G)$; для доказательства необходимости использовать упражнение 32а).)

§ 2. Упорядоченные поля

1. *Упорядоченные кольца*

Определение 1. *Пусть дано коммутативное кольцо A; говорят, что структура порядка на A согласована с кольцевой структурой, если она согласована со структурой аддитивной группы A и удовлетворяет следующей аксиоме*:

(УК) *Из неравенств $x \geqslant 0$ и $y \geqslant 0$ вытекает, что $xy \geqslant 0$.*

Кольцо A, снабженное такой структурой порядка, называется *упорядоченным кольцом*.

Примеры. 1) Кольца Q и Z, упорядоченные обычным образом, являются упорядоченными кольцами.

2) Произведение упорядоченных колец, снабженное структурой порядка произведения, является упорядоченным кольцом. В частности, кольцо A^E отображений множества E в упорядоченное кольцо A является упорядоченным кольцом.

В упорядоченном кольце из неравенств $x \geqslant y$ и $z \geqslant 0$ вытекает, что $xz \geqslant yz$. В самом деле, эти неравенства эквивалентны соответственно неравенствам $x - y \geqslant 0$, $z \geqslant 0$ и $(x - y)\, z \geqslant 0$. Этот результат показывает, что множество положительных

элементов упорядоченного кольца является мультипликативным упорядоченным моноидом.

Можно аналогично показать, что неравенства $x \leqslant 0$ и $y \geqslant 0$ (соответственно $y \leqslant 0$) влекут неравенство $xy \leqslant 0$ (соответственно $xy \geqslant 0$). Эти результаты обычно называют *правилом знаков*. Из них следует, что если A — *совершенно упорядоченное* кольцо, то всякий квадрат положителен, и, в частности, что всякий идемпотент (и единица, если она существует) положителен.

Пример. В кольце Z имеется *единственная* структура совершенно упорядоченного кольца, являющаяся обычной структурой: в самом деле, $1 > 0$, откуда по индукции $n > 0$ для каждого целого натурального $n \neq 0$. Кроме этой структуры, на Z существуют и другие структуры упорядоченного кольца, но уже не совершенно упорядоченного (см. ниже).

Замечание. Не следует думать, что всегда квадрат ненулевого элемента *строго* положителен, как это показывает пример кольца с нулевыми квадратами (гл. 1, § 8), заданного на аддитивной совершенно упорядоченной группе.

Пусть P — множество положительных элементов упорядоченного кольца A. Известно, что P определяет структуру порядка на A (§ 1, n° 3, предложение 3). Сказать, что A — упорядоченное кольцо — значит сказать, что P обладает следующими свойствами:

$$(AP_{\mathrm{I}})\ P+P \subset P,\ (AP_{\mathrm{II}})\ PP \subset P,\ (AP_{\mathrm{III}})\ P \cap (-P) = \{0\}.$$

В самом деле, условия (AP_{I}) и (AP_{II}) означают, что аддитивная группа кольца является упорядоченной группой (§ 1, n° 3, предложение 3), а условие (AP_{II}) совпадает с (УК). Напомним, что для того, чтобы отношение порядка, заданное на A, было *совершенным*, необходимо и достаточно следующее условие: $(AP_{\mathrm{IV}})\ P \cup (-P) = A$.

Пример. Если в Z в качестве P взять множество положительных (в обычном смысле) четных чисел, то мы получим структуру не совершенно упорядоченного кольца.

Напомним еще, что в абелевой совершенно упорядоченной группе из соотношения $nx = 0$ (для целого натурального $n \neq 0$) следует равенство $x = 0$ (§ 1, n° 3). Это дает нам следующий результат:

Предложение 1. *Всякое совершенно упорядоченное кольцо имеет характеристику нуль.*

2. Упорядоченные поля

Определение 2. *Поле, наделенное совершенной структурой порядка, называется упорядоченным полем, если структуры порядка и поля согласованы.*

Для полей мы ограничиваемся *совершенным* отношением порядка, так как другие случаи слишком «патологичны» (см. упражнение 5).

Примеры. 1) Поле Q рациональных чисел есть упорядоченное поле.

2) Подполе упорядоченного поля с индуцированной структурой порядка есть упорядоченное поле.

3) Поле действительных чисел есть упорядоченное поле.

В упорядоченных полях *правило знаков* можно уточнить следующим образом: если $x > 0$ и $y > 0$, то $xy > 0$ (в самом деле, $xy \neq 0$). Это показывает, что неравенство $x > 0$ эквивалентно $x^{-1} > 0$, поскольку $xx^{-1} = 1 > 0$. Строго положительные элементы поля образуют, следовательно, *мультипликативную совершенно упорядоченную группу*. С другой стороны, всякое упорядоченное поле имеет характеристику нуль (предложение 1).

Предложение 2. *Пусть A — совершенно упорядоченная область целостности, и пусть K — ее поле отношений. В K существует единственная структура порядка, индуцирующая на A заданную структуру и превращающая K в упорядоченное поле.*

Каждый элемент $x \in K$ записывается в виде $x = ab^{-1}$, где a и $b \in A$. Если x положителен, то a и b одинакового знака, и обратно. Следовательно, видно отсюда, что если на K существует отношение порядка, удовлетворяющее заданным условиям, то оно единственно, и множество положительных элементов P совпадает с множеством тех отношений ab^{-1}, у которых a и b — элементы из A одинакового знака. Остается, следовательно, показать, что P удовлетворяет условиям (AP_{I}), (AP_{II}), (AP_{III}) и (AP_{IV}). Это очевидно для (AP_{II}) и (AP_{IV}). Для проверки (AP_{I}) рассмотрим элемент $ab^{-1} + cd^{-1}$, где a, b, c, d мы можем считать положительными. Эта сумма записывается в виде $(ad + bc)(bd)^{-1}$, и $(ad + bc)$ и bd положительны.

Для проверки (AP_{III}) рассмотрим равенство вида $ab^{-1} = -cd^{-1}$, из которого следует, что $ad + bc = 0$. Если предположить, что

элементы a и b одного знака и то же самое для c и d, то правило знаков показывает, что ad и bc одинакового знака; отсюда вытекает, что $ad = bc = 0$ и $a = c = 0$; следовательно, множество P на самом деле удовлетворяет аксиоме (AP_{III}).

Пример. Поскольку Z допускает единственную структуру совершенно упорядоченного кольца, то поле Q допускает единственную структуру порядка, при которой Q — упорядоченное поле; это обычная структура порядка поля Q.

3. *Расширение упорядоченных полей*

Определение 3. *Пусть K — упорядоченное поле и E — некоторое расширение K. Говорят, что структура порядка на E определяет на E структуру упорядоченного расширения поля K, если она определяет на E структуру упорядоченного поля и если она индуцирует на K заданную структуру.*

Примеры. 1) Каждое упорядоченное поле K является упорядоченным расширением поля Q. В самом деле, так как K имеет характеристику нуль, оно является расширением поля Q. С другой стороны, как мы только что убедились, Q может быть упорядочено единственным образом.

2) Пусть K — упорядоченное поле, $K(X)$ — поле рациональных дробей от одной переменной над K. Определим структуру порядка в кольце многочленов $K[X]$, беря в качестве положительных элементов те многочлены, у которых старший коэффициент положителен. Полученное таким образом кольцо совершенно упорядочено, причем отношение порядка в нем является продолжением отношения порядка в K. Применяя предложение 2, определим в $K(X)$ структуру упорядоченного расширения поля K. Для $K = \mathbf{R}$ можно показать, что определенное таким образом на $K(X)$ отношение порядка совпадает с порядком роста в окрестности $+\infty$ (см. предложение 4, книга IV, гл. V).

Теорема 1. *Для того чтобы расширение E упорядоченного поля K допускало структуру упорядоченного расширения поля K, необходимо и достаточно, чтобы удовлетворялось следующее условие:*

(УР) *Из соотношения $p_1x_1^2 + \ldots + p_nx_n^2 = 0$ следуют равенства $p_1x_1 = p_2x_2 = \ldots = p_nx_n = 0$ для каждой конечной последовательности (x_i, p_i) пар, состоящих из элементов $x_i \in E$ и положительных элементов $p_i \in K$.*

Условие (УР), очевидно, эквивалентно условию (УР)′ — *1 не является суммой элементов вида* px^2, ($x \in E$, $p \in K$, $p \geqslant 0$). Условие является необходимым, поскольку элементы вида $p_i x_i^2$ положительны, а равенство $p_i x_i^2 = 0$ эквивалентно $p_i x_i = 0$.

Чтобы доказать достаточность условия, мы определим сейчас на E отношение порядка, построив часть $P \subset E$, удовлетворяющую условиям (AP_{I}), (AP_{II}), (AP_{III}) и (AP_{IV}), и содержащую множество K_+ положительных элементов поля K. Такая часть P действительно будет определять на E структуру упорядоченного расширения поля K, так как будет иметь место равенство $K \cap P = K_+$; в самом деле, если бы множество P содержало элемент $-a < 0$ из K, то элемент a принадлежал бы множеству $P \cap (-P)$, вопреки условию (AP_{III}).

Чтобы определить P, рассмотрим множество $\mathfrak{M}$ частей поля E, удовлетворяющих аксиомам (AP_{I}), (AP_{II}) и (AP_{III}) и содержащих объединение K_+ с множеством C квадратов элементов поля E. Это множество $\mathfrak{M}$ не пусто, так как оно содержит множество P_0 элементов вида $\sum_i p_i x_i^2$ (то, что P_0 удовлетворяет аксиоме (AP_{III}) немедленно следует из условия (УР)). Кроме того, $\mathfrak{M}$ является индуктивным. Поэтому в силу теоремы Цорна существует максимальный элемент $P \in \mathfrak{M}$, о котором нам остается доказать, что он удовлетворяет условию (AP_{IV}); а это вытекает из следующей леммы:

Лемма. *Пусть* $P \in \mathfrak{M}$ *и* $x \overline{\in} P$; *тогда существует такое множество* $P' \in \mathfrak{M}$, *что* $P \subset P'$ *и* $-x \in P'$.

Положим $P' = P - xP$ и убедимся, что P' обладает требуемыми свойствами. Так как $0 \in C \subset P$, то $P \subset P'$. Отсюда $C \in P'$ и $K_+ \subset P'$. Так как $1 \in C \subset P$, то $-x \in P'$. Имеем: $P' + P' = P - xP + P - xP = P + P - x(P + P) \subset P - xP = P'$, откуда следует условие (AP_{I}). Имеем далее: $P'P' = (P - xP) \times (P - xP) = PP + x^2PP - x(PP + PP) \subset P + CP - xP \subset P - xP = P'$, откуда следует (AP_{II}).

Проверим, наконец, свойство (AP_{III}): пусть имеется равенство $p - xq = -(r - xs)$, где p, q, r, s принадлежат p; отсюда следует $x(s + q) = p + r$, если $(s + q) \neq 0$, то $x = (s + q)^{-2}(s + q)(p + r) \subset CPP \subset P$ в противоречии с

предположением; следовательно, $s + q = 0$, откуда $p + r = 0$; так как P удовлетворяет (AP_{III}), то отсюда следует, что $s = q = r = p = 0$, чем доказательство заканчивается.

Следствие («теорема Артина — Шрайера»). *Для того чтобы в поле E существовала структура порядка, превращающая E в упорядоченное поле, необходимо и достаточно, чтобы из равенства $x_1^2 + \ldots + x_n^2 = 0$ вытекало, что $x_1 = x_2 = \ldots = x_n$.*

Необходимость очевидна. Обратно, из данного условия вытекает, что E имеет характеристику нуль и, следовательно, может рассматриваться как расширение поля Q; тогда имеет место условие (УР), и теорема 1 показывает, что в E можно определить структуру упорядоченного расширения поля Q, другими словами, структуру упорядоченного поля.

В поле E *не может* существовать структура упорядоченного поля, если -1 есть квадрат некоторого элемента. В частности, это справедливо для алгебраически замкнутого поля.

4. *Алгебраические расширения упорядоченных полей*

В этом параграфе (за исключением предложения 8), мы будем отождествлять для краткости многочлены и полиномиальные функции. Это не представит неудобства, так как поля коэффициентов имеют характеристику нуль и, следовательно, бесконечны (гл. IV, § 2, n° 5, предложение 9).

Пусть K — упорядоченное поле и f многочлен над K. Мы скажем, что f *меняет знак в* K, если существуют два элемента a, $b \in K$ такие, что $f(a)\,f(b) < 0$; говорят тогда, что f *меняет знак между* a *и* b.

Предложение 3. *Пусть K — упорядоченное поле и f — неприводимый над K многочлен, меняющий знак в K между a и b. Поле $E = K[X]/(f)$ допускает тогда структуру упорядоченного расширения поля K.*

Доказательство проведем индукцией по степени n многочлена f. При $n = 1$ имеем $E = K$, и утверждение тривиально. Пусть наше утверждение справедливо для всех степеней $\leqslant n-1$. Методом от противного докажем, что оно справедливо для n. В силу (УР)′ мы можем предположить, что справедливо неко-

торое соотношение вида

$$1+\sum_i p_i f_i^2(X) \equiv 0 \pmod{f(X)}, \quad \text{где} \quad f_i \in K[X] \quad \text{и} \quad p_i \in K_+.$$

Без ограничения общности можно считать, что степени многочленов f_i не превосходят $n-1$ (гл. V, § 3, теорема 1). Имеем тогда

$$1+\sum_i p_i f_i^2(X) = h(X) f(X),$$

где $h \neq 0$ — многочлен, степень которого не превосходит $n-2$. Заменяя в предыдущем равенстве X на a и b, видим, что $h(b) f(b) > 0$ и $h(a) f(a) > 0$. Так как, согласно предположению, многочлен f меняет знак между a и b, то $h(a) h(b) < 0$. Тогда неравенство того же вида выполняется для одного из неприводимых множителей $g(X)$ многочлена $h(X)$: $g(a) g(b) < 0$. Но $1+\sum_i p_i f_i^2(X) \equiv 0 \pmod{g(X)}$, а это означает, что в поле $K[X]/(g)$ нельзя ввести структуру упорядоченного расширения поля K (теорема 1), что противоречит предположению индукции.

Замечание. Над упорядоченным полем K могут существовать неприводимые многочлены f, не меняющие знака в K, но такие, что поле $K[X]/(f)$ обладает структурой упорядоченного расширения поля K (см. упражнение 17в)).

Для применения предыдущего предложения нам понадобится следующий результат:

Предложение 4. *Пусть K — упорядоченное поле и f — многочлен над K. Существует интервал в K, вне которого f имеет тот же знак, что и его старший член.*

Все легко сводится к случаю, когда f — унитарный многочлен; тогда можно записать $f(x) = x^n(1 + a_1 x^{-1} + \ldots + a_n x^{-n})$. Пусть

$$M = \sup(1, |a_1| + \ldots + |a_n|).$$

При $|x| > M$ имеем $1 + a_1 x^{-1} + \ldots + a_n x^{-n} > 0$. Отсюда следует утверждение.

Следствие 1. *Каждое алгебраическое расширение нечетной степени упорядоченного поля допускает структуру упорядоченного расширения.*

Каждое такое расширение, будучи простым (гл. V, § 7, n° 7, предложение 12), изоморфно полю вида $K[X]/(f)$, где f — непри-

водимый многочлен нечетной степени. Достаточно показать, что f меняет знак (предложение 3), что немедленно следует из предложения 4.

Следствие 2. *Если a — положительный элемент упорядоченного поля K, то поле корней многочлена $x^2 - a$ допускает структуру упорядоченного расширения поля K.*

Утверждение тривиально, если a — квадрат в K. Если это не так, то $x^2 - a$ — неприводимый многочлен, меняющий знак, поскольку он < 0 при $x = 0$ и имеет знак x^2, т. е. > 0, вне некоторого интервала из K. А тогда достаточно применить предложение 3.

Замечание. Если упорядоченное поле K содержит «квадратные корни» из некоторого положительного элемента a (корни многочлена $x^2 - a$), то в общем случае под $\sqrt{a}$ понимается положительный корень. Если поле K *не* содержит квадратных корней b и $-b$ из элемента a, то поле корней многочлена $x^2 - a$ допускает *две* структуры упорядоченного расширения поля K, причем одно получается из другого K-автоморфизмом, определенным отображением $b \to -b$; выбор одной из этих структур порядка определяет тогда $\sqrt{a}$; это будет тот из элементов b, $-b$, который положителен.

Если a и a' — два положительных элемента из K, квадратные корни которых лежат в K, то $\sqrt{aa'} = (\sqrt{a})(\sqrt{a'})$, как это следует из определения корня и правила знаков.

5. *Максимальные упорядоченные поля*

Определение 4. *Упорядоченное поле K называется максимальным, если каждое алгебраическое упорядоченное расширение поля K совпадает с K.*

Пример. Мы увидим дальше (Общ. топол., гл. VIII), что поле R действительных чисел является максимальным упорядоченным полем.

Существование максимальных упорядоченных полей вытекает из следующей теоремы:

Теорема 2. *Каждое упорядоченное поле K обладает упорядоченным алгебраическим расширением, которое является максимальным упорядоченным полем.*

Можно показать, что это последнее поле определяется с точностью до K-изоморфизма *).

Пусть Ω — алгебраическое замыкание поля K, и пусть $\mathfrak{N}$ — множество упорядоченных расширений поля K, содержащихся в Ω. Упорядочим множество $\mathfrak{N}$ с помощью отношения «L является упорядоченным расширением поля M». Упорядоченное множество $\mathfrak{N}$, снабженное этой структурой порядка, будет *индуктивным*: в самом деле, если (L_ι) вполне упорядоченное семейство элементов из $\mathfrak{N}$, то поле $L = \bigcup_\iota L_\iota$ можно упорядочить, взяв $L_+ = \bigcup_\iota (L_\iota)_+$, а тогда L — верхняя грань семейства L_ι (см. гл. V, § 2, предложение 3). В силу теоремы Цорна $\mathfrak{N}$ содержит максимальный элемент E, удовлетворяющий требованию теоремы.

Предложение 5. *Пусть K — максимальное упорядоченное поле и f — многочлен из $K[X]$, меняющий знак между двумя элементами a и b из K. Тогда f имеет в поле K такой корень x, что $a < x < b$.*

По крайней мере один из неприводимых множителей многочлена f меняет знак между a и b; пусть это будет h. Поле $K[X]/(h)$ обладает тогда структурой упорядоченного расширения поля K. Следовательно, оно совпадает с K и h имеет степень 1. Так как $h(a)\,h(b) < 0$, единственный корень x многочлена h удовлетворяет неравенству $a < x < b$, поскольку многочлен первой степени является монотонной функцией.

Предложение 5 дает, в частности,

Предложение 6. *Каждый положительный элемент максимального упорядоченного поля K имеет в K квадратный корень. Каждый многочлен нечетной степени над K имеет по крайней мере один корень в K.*

Это непосредственно следует из следствий 2 и 1 предложения 4.

Следствие. *Максимальное упорядоченное поле K не допускает иных, кроме имеющейся, структур порядка, согласованных со структурой поля.*

В самом деле, положительные элементы поля K определяются его алгебраической структурой: они являются квадратами.

*) Смотри Ван-дер-Варден, Современная алгебра, 1-е изд., т. 1.

6. *Характеризация максимальных упорядоченных полей. Теорема Эйлера—Лагранжа*

Свойство, установленное в предложении 6, характеризует максимальные упорядоченные поля. Более точно:

Теорема 3 (Эйлер — Лагранж). *Пусть K — упорядоченное поле. Следующие три свойства эквивалентны:*

а) *Поле $K(i)$ алгебраически замкнуто (i один из квадратных корней из -1).*

б) *Поле K является максимальным упорядоченным полем.*

в) *Каждый положительный элемент в K является квадратом, и каждый многочлен над K нечетной степени имеет корень в K.*

Ясно, что а) влечет б): в самом деле, K обладает, с точностью до изоморфизма, двумя алгебраическими расширениями: самим K и $K(i)$. Последнее не может быть упорядоченным, так как -1 является в нем квадратом.

Для доказательства импликации б) → в) нужно лишь применить предложение 6. Остается показать, что из в) вытекает а). Это является результатом двух следующих предложений:

Предложение 7. *Пусть K—упорядоченное поле, каждый положительный элемент которого есть квадрат. Тогда каждый элемент поля $K(i)$ есть квадрат и каждый многочлен над K (i) второй степени имеет корень в K (i).*

Покажем сначала, что второе утверждение следует из первого. Многочлен второй степени $ax^2 + bx + c$ можно записать в следующей форме, которая часто называется *канонической формой трехчлена*:

$$a\left(\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right).$$

Если d — квадратный корень из $(b^2 - 4ac)/4a^2$, то $d - (b/2a)$ есть корень заданного многочлена второй степени.

Покажем теперь, что каждый элемент $a + b_i (a \in K,\ b \in K)$ является квадратом. Найдем такой элемент $x + y_i$, что $(x + y_i)^2 = a + b_i$; это равенство можно записать в виде двух таких равенств: $x^2 - y^2 = a$ и $2xy = b$. Отсюда получаем

$$(x^2+y^2)=a^2+b^2.$$

Обозначая через c положительный квадратный корень из $a^2 + b^2$, получаем $c \geqslant |a|$, $c \geqslant |b|$ и $x^2 + y^2 = c$. Отсюда $x^2 = (c + a)/2$ и $y^2 = (c - a)/2$. Так как $c \geqslant |a|$, то эти уравнения разрешимы в K, и если x_0 и y_0 — одно из решений, то $x_0^2 - y_0^2 = 0$ и $2x_0y_0 = \pm b$. Взяв $x = x_0$ и $y = b/2x_0$, получим искомый квадратный корень.

Предложение 8. *Пусть K — поле* (произвольной характеристики). *Пусть K и $K' = K(i)$ таковы, что:*

а) *каждый многочлен нечетной степени над K имеет корень в K,*

б) *каждый многочлен второй степени над K' имеет корень в K'. Тогда K' алгебраически замкнуто.*

Обозначим через $\bar{a}$ элемент, сопряженный с элементом $a \in K'$, другими словами, образ a при K-автоморфизме поля K', определенном отображением $i \to -i$. Для каждого многочлена f над K' обозначим через $\bar{f}$ многочлен, все коэффициенты которого сопряжены с коэффициентами многочлена f. Достаточно показать, что каждый многочлен над K имеет корень в K'. В самом деле, пусть f — многочлен над K'; тогда многочлен над K $g = f\bar{f}$ имеет корень в K', который будет корнем либо для f, либо для $\bar{f}$. В этом последнем случае элемент, сопряженный с этим корнем, будет корнем для f.

Пусть теперь f — многочлен над K степени $2^n p$, где p нечетно. При $n = 0$, в силу условия а), f имеет корень в K. Проведем доказательство индукцией по n. Пусть E — расширение поля K, в котором f разлагается на линейные множители: $f(X) = \prod_i (X - a_i)$. Пусть $b \in K$; образуем многочлен h, корнями которого являются элементы

$$y_{ij} = a_i + a_j + ba_ia_j \qquad (i > j).$$

Коэффициентами этого многочлена будут симметрические функции от переменных a_i с коэффициентами из K; следовательно, h — многочлен над K (гл. V, Приложение 1); так как он имеет степень $2^n p(2^n p - 1)/2 = 2^{n-1}p'$ (p нечетно), то он имеет корень y_{ij}, лежащий в K', в силу предположения индукции. Если принять во внимание, что это верно для каждого $b \in K$ и что K — бесконечное поле (в самом деле, конечное поле, имеющее

произвольно большие простые расширения нечетной степени (гл. V, § 11, предложение 3), не может удовлетворить условию а)), то отсюда следует существование по крайней мере одной пары (ij) такой, что $a_i + a_j + ba_ia_j \in K'$ и $a_i + a_j + b'a_ia_j \in K'$, где $b \neq b'$. Тогда элементы $a_i + a_j$ и a_ia_j лежат в K', и, следовательно, a_i и a_j — элементы из K', поскольку они являются корнями уравнения второй степени $x^2 - (a_i + a_j)\,x + a_ia_j = 0$. Это доказывает требуемое.

Пусть K — упорядоченное поле, и пусть $K' = K(i)$; для каждого элемента $z = a + bi \in K'$ *норма* $z\bar{z} = a^2 + b^2$ элемента z над полем K (гл. V, § 10, n° 6) является положительным элементом поля K, который равен нулю лишь при $z = 0$. Если в K каждый положительный элемент является квадратом (если, в частности, K — максимальное упорядоченное поле), назовем *абсолютным значением элемента* z и обозначим через $|z|$ положительный квадратный корень из нормы $z\bar{z}$. Так как $|zz'|^2 = |z|^2\,|z'|^2$, то $|zz'| = |z|\,|z'|$.

Кроме того, имеет место *неравенство треугольника*

$$|z+z'| \leqslant |z| + |z'|$$

для каждой пары элементов z, $z' \in K'$. В самом деле, если $z = a + bi$, $z' = a' + b'i$, это неравенство эквивалентно следующему:

$$(a+a')^2 + (b+b')^2 \leqslant a^2 + b^2 + a'^2 + b'^2 + 2\sqrt{(a^2+b^2)(a'^2+b'^2)};$$

или еще:

$$(aa' + bb')^2 \leqslant (a^2+b^2)(a'^2+b'^2),$$

которое записывается в виде $(ab' - ba')^2 \geqslant 0$.

Теорема 3 позволяет нам найти все неприводимые многочлены над максимальным упорядоченным полем.

Предложение 9. *Если K — максимальное упорядоченное поле, то единственными неприводимыми над K многочленами являются многочлены первой степени и многочлены второй степени $ax^2 + bx + c$, у которых $b^2 - 4ac < 0$.*

Так как поле $K(i)$ алгебраически замкнуто, каждое алгебраическое расширение поля K имеет либо первую, либо вторую степень, и следовательно, лишь многочлены первой или второй степени могут быть неприводимыми над K. Чтобы увидеть, какие из многочленов второй степени неприводимы, достаточно написать каноническую форму трехчлена $a\,((x + (b/2a))^2 - (b^2 - 4ac)/4a^2)$ (ср. предложение 7).

З а м е ч а н и е. Рассмотрение канонической формы трехчленов дает более сильный результат: пусть K — упорядоченное поле; для того чтобы многочлен второй степени над K $ax^2 + bx + c$ имел в K постоянный знак, необходимо и достаточно, чтобы $b^2 - 4ac < 0$, и знак многочлена в этом случае совпадет со знаком a.

У п р а ж н е н и я. 1) Пусть A — совершенно упорядоченное кольцо и B — подкольцо в A.

а) Элемент $x \in A$ называется *бесконечно большим* относительно B, если $|y| < |x|$ для каждого $y \in B$. Показать, что множество элементов из A, не являющихся бесконечно большими относительно B, образуют подкольцо $F(B)$ в A, содержащее B.

б) Элемент $x \in A$ называется *бесконечно малым* относительно B, если $|x| < y$ для каждого $y \in B$, $y > 0$. Если кольцо A обладает единицей, принадлежащей B, и если для каждого $y \in B$ такого, что $0 < y$, существует такой элемент $z \in B$, что $0 < z < y$, то множество элементов из A, бесконечно малых относительно B, образует подкольцо $I(B)$ в A. Если, кроме того, для каждой пары таких элементов y, z из B, что $0 < y < z$, существует такой элемент $x \in B$, что $0 < xz < y$, то $I(B)$ является *идеалом* в $F(B)$.

2) Пусть A — совершенно упорядоченное кольцо. Пусть $\mathfrak{n}$ — множество нильпотентных элементов из A (являющееся идеалом в A); каждый элемент кольца A, не принадлежащий $\mathfrak{n}$, является бесконечно большим относительно $\mathfrak{n}$. Фактор-кольцо $A/\mathfrak{n}$ совершенно упорядочено (§ 1, упражнение 4) и не имеет делителей нуля.

3) Пусть P — множество элементов поля Q, образованное нулем и рациональными числами, не меньшими (в обычном смысле) чем единица. Показать, что P удовлетворяет аксиомам (AP_{I}), (AP_{II}) и (AP_{III}).

*4) а) Пусть K — поле, P — часть из K, удовлетворяющая условиям (AP_{I}) (AP_{II}) и (AP_{III}) и такая, что $K^2 \subset P$ (где K^2 — множество квадратов элементов из K); показать, что если $x > 0$ при структуре порядка, определенной множеством P, то $x^{-1} > 0$; вывести отсюда, что множество K_+^* строго положительных элементов из K является подгруппой мультипликативной группы поля K.

б) В поле Q единственным множеством P, удовлетворяющим условию а), является множество тех рациональных чисел, которые $\geqslant 0$ (при обычном порядке).

в) Пусть P — часть в K, удовлетворяющая условиям (AP_{I}), (AP_{II}), (AP_{III}), такая, что $1 \in P$, и пусть при порядке, определенном множеством P, из первенства $x > 0$ следует, что $x^{-1} > 0$. Показать, что для положительных y и z из $y^2 \geqslant z^2$ следует, что $y \geqslant z$. Вывести отсюда, что для любого $y > 0$ $\frac{1}{2}(y + y^{-1}) \geqslant 1 - n^{-1}$ для каждого целого $n > 0$. (Заметить, что $(y + y^{-1})^{2m} \geqslant \binom{2m}{m}$ для всякого целого

$m > 0$.) Вывести отсюда, что если структура порядка аддитивной группы поля K, определенная множеством P, архимедова (§ 1, упражнение 31), то $(y - z)^2 \geqslant 0$ для каждой пары y, z элементов из P; если K' — подполе в K, порожденное множеством P, то $x^2 \geqslant 0$ для каждого $x \in K'$.

г) Пусть $K = R(X)$ — поле рациональных дробей от одного переменного над полем R; пусть P — множество, образованное нулем и теми рациональными дробями $u \in K$, для которых при каждом действительном числе t значение $u(t)$ определено и больше нуля. Показать, что P удовлетворяет условиям в) и порождает K, но что существует такой элемент $v \in K$, что $v^2 \notin P$.

5) Пусть K — поле, P — его часть, определяющая в K структуру *решеточной* упорядоченности, согласованную с кольцевой структурой поля K.

а) Показать, что если $x \neq 0$ — такой элемент, что $(x^+)^{-1} > 0$, то $(x^+x)^+ = (x^+)^2$.

б) Вывести отсюда, что если неравенство $x > 0$ влечет неравенство $x^{-1} > 0$, то K совершенно упорядочено.

6) Поле $K = Q(X)$ рациональных дробей от одной переменной над полем Q порождается множеством K^2 своих квадратов. Показать, что множество P сумм квадратов элементов из K определяет не решеточную упорядоченность, согласованную с кольцевой структурой поля K, при которой из $u > 0$ следует, что $u^{-1} > 0$.

7) Для того чтобы в поле K, имеющем характеристику $\neq 2$, каждый элемент был равен сумме квадратов некоторых элементов, необходимо и достаточно, чтобы -1 представлялась в виде суммы квадратов. (Заметить, что каждый элемент из K есть разность двух квадратов.)

*8) Пусть A — непустая часть поля K характеристики, отличной от 2; поле K называется *A-упорядочиваемым*, если ни один элемент из A не является суммой квадратов элементов из K. Поле K называется *упорядочиваемым*, если на K можно ввести совершенную структуру порядка, согласованную с кольцевой структурой поля K.

а) Показать, что если поле K A-упорядочиваемое, то оно упорядочиваемо и, следовательно, имеет характеристику нуль.

б) Показать, что всякое алгебраическое расширение и всякое чистое расширение нечетных степеней A-упорядочиваемого поля K сами являются A-упорядочиваемыми полями (рассуждать как в предложении 3).

в) Пусть K — A-упорядочиваемое поле и пусть элемент $b \in K$ не может быть представлен в виде $ca - d$, где $a \in A$, а c и d — суммы квадратов элементов из K. Показать, что поле $K(\sqrt{b})$ A-упорядочиваемо.

г) Поле K называется *максимальным A-упорядочиваемым*, если не существует отличного от K алгебраического расширения поля K,

являющегося A-упорядочиваемым. Показать, что максимальное A-упорядочиваемое поле K обладает следующими свойствами: 1° поле K *пифагорово*, т. е. каждая сумма квадратов элементов из K есть квадрат; 2° ни один элемент из A не является квадратом; 3° каждый элемент из K, не являющийся квадратом, представим в виде $c^2a - d^2$, где $a \in A$; 4° каждый многочлен из $K[X]$ нечетной степени имеет в K по крайней мере один корень (использовать б) и в)).

д) Показать, что если поле K удовлетворяет четырем условиям г), то каждый алгебраический над K элемент является элементом 2^q-й степени над K. (Рассуждать, как в предложении 8 индукцией по экспоненте 2 в степени рассматриваемого элемента.) Показать, с другой стороны, что никакое квадратичное расширение поля K не является A-упорядочиваемым. Вывести отсюда, что поле K является максимальным A-упорядочиваемым *).

е) Пусть K — A-упорядочиваемое поле, Ω — алгебраически замкнутое расширение поля K. Показать, что существует максимальное A-упорядочиваемое поле R, содержащееся в Ω и содержащее K. (Использовать б), в) и д).)

9) Пусть q — целое натуральное число, не являющееся квадратом; в поле $K = Q(\sqrt{q})$ пусть A состоит из -1 из $\sqrt{q}$; показать, что поле K A-упорядочиваемо. Показать, что существует алгебраическое расширение E поля K, являющееся упорядочиваемым, пифагоровым и таким, что каждый многочлен над E нечетной степени имеет в поле E корень, но что в E нельзя ввести структуру максимального упорядоченного поля. (Рассмотреть максимальное A-упорядочиваемое расширение поля K.)

*10) а) Пусть K — упорядочиваемое поле, E — его расширение Галуа. Показать, что либо E упорядочиваемо, либо существует упорядочиваемое алгебраическое расширение F поля K, содержащееся в E и такое, что E является квадратичным расширением поля F. (Использовать теорему 1, гл. V, § 10).

б) Показать, что многочлен $X^4 + 2$ неприводим под Q и что если K — расширение 4-й степени поля Q, получаемое присоединением к Q корня этого многочлена, то K не содержит никакого упорядочиваемого подполя, отличного от Q. (Определить подполя поля K с помощью теории Галуа.)

11) Пусть K — упорядоченное поле и G — его подполе:

а) Показать, что для того, чтобы элемент $x \neq 0$ был бесконечно большим относительно G (упражнение 1), необходимо и достаточно,

*) Использовать теорию Галуа и следующий результат теории групп: пусть дана конечная группа Γ порядка p^q, где p — простое число, и подгруппа $\Delta \neq \Gamma$ группы Γ; тогда существует подгруппа Δ_0 группы Γ порядка p^{q-1}, содержащая Δ (см. H. Zassenhaus, The theory of groups, New York, Chelse Publ. Co., 1949, стр. 107 (см. также М. Холл, Теория групп, ИЛ, Москва, 1962, стр. 59. (*Прим. перев.*)).

чтобы x^{-1} был бесконечно малым относительно G. Говорят, что поле K *сравнимо* с G, если в K не существует бесконечно большого относительно G элемента (и, следовательно, не существует отличного от нуля бесконечно малого относительно G элемента). Для того чтобы поле K было сравнимо со своим простым подполем Q, необходимо и достаточно, чтобы аддитивная группа поля K была *архимедова* (§ 1, упражнение 31) и, следовательно, чтобы K было изоморфно подполю поля R (§ 1, упражнение 33 в)).

б) Показать, что в кольце $F(G)$ элементов из K, не являющихся бесконечно большими относительно G, множество $I(G)$ бесконечно малых относительно G элементов является максимальным идеалом; кроме того, структура порядка в факторкольце $K(G) = F(G)/I(G)$, индуцированная структурой порядка кольца $F(G)$ (§ 1, упражнение 4), совершенна и согласована с кольцевой структурой.

в) Показать, что каждый класс по mod $I(G)$ может содержать лишь один элемент из G. Вывести отсюда, что каноническое отображение поля G в $K(G)$ является изоморфизмом упорядоченного поля G на подполе G' упорядоченного поля $K(G)$ и что $K(G)$ *сравнимо с* G'.

12) Пусть K — максимальное упорядоченное поле, f — многочлен над K, a и b — два корня многочлена f в K такие, что $a < b$ и f не имеет корней между a и b. Показать, что если g — рациональная дробь над K, знаменатель которой не обращается в нуль при $a \ll x \ll b$, то уравнение $f(x)\,g(x) + f'(x) = 0$ имеет нечетное число корней в (a, b) (использовать предложение 5). Вывести отсюда, что если h — рациональная дробь над K, обращающаяся в нуль между a и b, знаменатель которой не равен нулю в (a, b), то уравнение $h'(x) = 0$ имеет по крайней мере один корень в (a, b) («теорема Ролля»).

13) Пусть K — максимальное упорядоченное поле, h — рациональная дробь над K, $[a, b]$ — замкнутый интервал, в котором h всюду определена. Показать, что существует такой элемент $c \in (a, b)$, что $h(b) - h(a) = (b - a)\,h'(c)$ («теорема о среднем»; использовать «теорему Ролля», см. упражнение 12). Вывести отсюда, что для того, чтобы $h(x)$ был возрастающей функцией в $[a, b]$, необходимо и достаточно, чтобы выполнялось неравенство $h'(x) \geqslant 0$ в этом интервале (для доказательства необходимости разбить этот интервал корнями уравнения $h'(x) = 0$).

*14) а) Пусть K — максимальное упорядоченное поле, E — подполе в K и f — многочлен над E; показать, что все корни многочлена f, лежащие в K, принадлежат $F(E)$ (упражнение 11б)) (использовать предложение 4). Вывести отсюда, что если G — подполе в K и $E \subset K$ — расширение поля G, сравнимое с G (упражнение 11), то множество элементов из K, алгебраических над E, образует максимальное упорядоченное поле, сравнимое с G.

б) Вывести из а), что поле $K(G)$ (упражнение 11) при условиях упражнения 14 а) является максимальным упорядоченным полем.

в) Пусть f — многочлен над G степени $\geqslant 1$. Доказать, что для того, чтобы элемент $f(t)$ был бесконечно большим относительно G, необходимо и достаточно, чтобы элемент t был бесконечно большим относительно G; для того чтобы (t) был бесконечно малым относительно G, необходимо и достаточно, чтобы t было равно (mod $I(G)$) корню многочлена f в K. (Разбить K на интервалы корнями многочленов f и f', лежащими в K, и использовать упражнение 13; заметить, что если $x < t$ и элемент $x \in K$ несравним (mod $I(G)$) с t, то существует такой $y \in K$, что $x < y < t$ и $y - x \in G$.)

*15) Пусть K — максимальное упорядоченное поле. Рассмотрим в поле рациональных дробей $K(X)$ структуру порядка, при которой $K(X)$ является упорядоченным расширением поля K. Показать, что эта структура определяется множеством A тех $x \in K$, которые меньше X (показать, что знак каждого многочлена f над K определяется множеством A, используя предложение 9). Обратно, показать, что каждому множеству $A \subset K$ такому, что из $x \in A$ и $y \leqslant x$ вытекает, что $y \in A$, соответствует на $K(X)$ структура упорядоченного расширения, при которой A совпадает с множеством тех $x \in K$, которые меньше X (тем же методом). Если A обладает наибольшим элементом, или CA наименьшим элементом, либо если $A = K$ или $A = \phi$, то структура порядка, определяемая на $K(X)$ множеством A, такова, что $K(X)$ несравнимо с K. Если, наоборот, A и CA не пусты и если не существует ни наибольшего элемента в A, ни наименьшего элемента в CA, то поле $K(X)$ сравнимо с K.

16) Используя упражнение 15, дать пример поля E, наделенного несколькими структурами упорядоченных полей, которые не могут быть получены одна из другой с помощью автоморфизма поля E. Используя это, дать пример поля E, наделенного структурой порядка, согласованной с кольцевой структурой, но при которой E не решеточно-упорядочено (рассмотреть диагональ множества $E \times E$ и использовать упражнение 5).

*17) а) Если K — архимедовски упорядоченное поле (упражнение 11а)), x и y — два элемента из K такие, что $x < y$, показать, что существует такое число $r \in Q$, что $x < r < y$. °Вывести отсюда, что не существует других упорядоченных подполей поля R, изоморфных K.°

б) В поле $K = Q(X)$ рассмотрим структуру порядка, при которой $X > 0$ и X бесконечно велик относительно Q (упражнение 15). Показать, что поле K сравнимо со своим подполем $Q(X^2)$ и дать пример двух элементов x, y из K таких, что $x < y$, и не существует элемента из $Q(X^2)$, лежащего между x и y.

в) Пусть K — упорядоченное поле, определенное в б); показать, что многочлен $f(Y) = (Y^2 - X)(Y^2 - 4X) - 1$ над K неприводим, но обладает корнями в каждом максимальном упорядоченном расширении поля K и что $f(a) > 0$ для всех $a \in K$.

*18) Пусть K — упорядоченное поле, E — чистое расширение поля K, $(X_\iota)_{\iota\in I}$ — чистый базис расширения E (гл. V, § 5, определение 1).

а) Если поле K архимедово, то для того, чтобы в E можно было ввести структуру упорядоченного расширения поля K, при которой E сравнимо с K, необходимо и достаточно, чтобы мощность множества I была не больше мощности базиса трансцендентности поля R над K (где K рассматривается как подполе поля R; см. упражнение 17а)). Множество всех таких структур тогда эквивалентно множеству взаимно однозначных отображений f множества I в R таких, что $f(I)$ — алгебраически свободная система над K.

б) Если поле K не архимедово, то на E всегда существует по крайней мере одна такая структура упорядоченного расширения поля K, что E сравнимо с K. (Когда I состоит из одного элемента, использовать упражнение 15, замечая, что Q не может иметь верхнюю грань в K; распространить на общий случай с помощью теоремы Цорна.)

19) °Пусть K — подполе в R, θ — действительное число, алгебраическое над K. Показать, что число структур упорядоченного расширения в поле $K(\theta)$ над K равно количеству действительных чисел, сопряженных с θ (использовать упражнение 14а) и 17а)).

*20) Пусть K — максимальное упорядоченное поле, G — подполе в K. Показать, что множество расширений поля G, сравнимых с G и содержащихся в K, индуктивно; если E_0 — максимальный элемент этого множества, показать, что E_0 изоморфно полю $K(G)$, определенному в упражнении 11 б) (доказать, что каноническое отображение $F(G)$ на $K(G)$ отображает E_0 на $K(G)$, установив вначале при помощи упражнения 14а), что E_0 — максимальное упорядоченное поле, потом с помощью упражнения 15, что в $K(G)$ не существует элемента, трансцендентного над каноническим образом поля E_0).

21) а) Пусть K — максимальное упорядоченное поле, m и M — два элемента из K, причем $m < M$. Показать, что каждый многочлен $f \in K(X)$, положительный в интервале $[m, M]$, представим в виде суммы многочленов вида $(\alpha X + \beta)\, g^2$, где $g \in K[X]$, а многочлен $\alpha X + \beta$ положителен в $[m, M]$. (Для многочленов первой степени это очевидно, а для многочленов второй степени можно воспользоваться следующими формулами:

$$(X-a)(X-b) = (X-b)^2 + (b-a)(X-b),$$

$$(X-a)(b-X) = ((X-a)(b-X)^2 + (b-X)(X-a)^2)/(b-a)$$

при $a < b$.)

б) Показать, что результат упражнения а) не всегда справедлив, если K — произвольное упорядоченное поле. (Заметить, что многочлен может быть положителен в K, но не в максимальном упорядоченном расширении поля K; см. упражнение 17в).)

*22) а) Пусть E — алгебраическое замыкание поля K, являющееся расширением поля K степени q ,где q — простое число. Показать, что поле K совершенно (гл. V, § 8, n° 1).

б) Показать, что q не равно характеристике поля K (гл. V, § 11, упражнение 9б)).

в) Показать, что K содержит корни q-й степени из 1, и что E является полем корней неприводимого над K многочлена $X^q - a$; вывести отсюда, что $q = 2$ (в противном случае из упражнения 12, § 11, гл. V следует, что $X^{q^2} - a$ неприводим). Показать, кроме того, что $-a$ является квадратом в K (упражнение 12, § 11, гл. V), но что -1 не является квадратом в K и что $E = K(i)$ ($i^2 = -1$).

г) Предположим теперь, что K таково, что его алгебраическое замыкание E имеет конечную, отличную от 1 степень над K. Показать, что $i \notin K$ и что $E = K(i)$ (если $E \neq K(i)$, то из теории Галуа следовало бы, что существует такое поле F, что $K(i) \subset F \subset E$ и что E имеет простую степень над F; применить в)).

Вывести отсюда, что K максимальное упорядочиваемое поле (следовательно, в нем можно ввести некоторую структуру максимального упорядоченного поля) (показать индукцией по n, что каждая сумма n квадратов элементов из K является квадратом элемента из K; для доказательства того, что $a^2 + b^2$ является квадратом, рассмотреть квадратные корни $x + iy$ из элементов $a + ib$ в поле $K(i)$).

*23) Пусть K — *некоммутативное* тело.

а) Показать, что если часть $P \subset K$ удовлетворяет условиям (AP_{I}), (AP_{II}), (AP_{III}) и (AP_{IV}), то свойства упорядоченных полей, изложенные в n° 1 и 2, распространяются на «некоммутативное упорядоченное тело» K, и что P содержит множество C сумм произведений квадратов элементов из K.

б) Показать, что P содержит коммутаторы $xyx^{-1}y^{-1}$ элементов из K (показать, что каждый коммутатор есть произведение квадратов; заметить, что в факторгруппе G группы K^* по подгруппе произведений квадратов каждый элемент имеет порядок 2, и следовательно, G абелева).

в) Показать, что если -1 не является суммой произведений квадратов, то в K существует часть P, удовлетворяющая условиям (AP_{I}), (AP_{II}), (AP_{III}) и (AP_{IV}) (следуя доказательству теоремы 1).

г) Пусть G — упорядоченное поле и σ — отличный от тождественного автоморфизм поля G. Рассмотрим (некоммутативное) тело K «формальных левых рядов» $\sum_{n=-h}^{\infty} a_n X^n$ ($a_n \in G$), где $X^n a = \sigma^n(a)\, X^n$ (гл. IV, § 5, упражнение 10г)). Пусть σ отображает каждый положительный элемент из G в положительный элемент; показать, что множество P тех элементов из K, ненулевые члены наименьшей степени которых имеют положительный в G коэффициент, удовлетворяет условиям (AP_{I}), (AP_{II}), (AP_{III}), (AP_{IV}) и определяет в K структуру

упорядоченного некоммутативного тела. Показать, что в качестве поля G можно взять поле (обычных) формальных степенных рядов $Q((Y))$, а в качестве положительных элементов этого поля — множество формальных рядов $\sum_{n=-h}^{\infty} r_n Y^n$, ненулевые коэффициенты в членах наименьшей степени которых положительны; автоморфизм σ определим с помощью равенства $\sigma(Y) = 2Y$; тогда тело K называется «телом формальных рядов Гильберта».

°д) Показать, что некоммутативное тело не может быть архимедовски упорядоченным (применить предложение 1 Общ. топол., гл. V, § 2 к мультипликативной группе положительных элементов тела).$_\circ$

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

	Глава	§	n°
$N^{(I)}$	IV	1	1
X_ι (переменная)	IV	1	1
$A[X_\iota]_{\iota \in I}$, $A[X_{i_1}, X_{i_2}, \ldots, X_{i_p}]$	IV	1	1
$A[X]$, $A[X, Y, Z]$, $A[X_\iota]_{\iota \in \varnothing}$	IV	1	2
$\deg u$, $\deg_\varkappa u$ (u — ненулевой многочлен)	IV	1	3
$f(x)$ (f — многочлен одной переменной)	IV	2	1
$f[x]$, $f((x_\iota))$, $f(x_{i_1}, \ldots, x_{i_p})$ (f — многочлен, x_ι — попарно перестановочные элементы)	IV	2	2
$A[x]$, $A[x_\iota]_{\iota \in I}$, $A[x_{i_1}, x_{i_2}, \ldots, x_{i_l}]$, $A[M]$	IV	2	1
$f((X_\iota))$, $f(X_1, X_2, \ldots, X_n)$ (f — многочлен, X_ι — переменные)	IV	2	2
$F(f$ — многочлен)	IV	2	3
$K(X_\iota)_{\iota \in I}$, $K(X_1, X_2, \ldots, X_n)$	IV	3	1
$f(x)$, $f((x_\iota))$ (f — рациональная дробь, $X = (x_\iota)$ — семейство, допускающее подстановку в f)	IV	3	2
$K(x)$, $K(x_\iota)_{\iota \in I}$, $K(x_1, x_2, \ldots, x_n)$, $K(M)$	IV	3	2
$f((X_\iota))$, $f(X_1, X_2, \ldots, X_n)$ (f — рациональная дробь, X_i — переменные)	IV	3	3
Δf, $\Delta f(X_1, \ldots, X_p; Y_1, \ldots, Y_p)$ (f — многочлен)	IV	4	1
df, $df(X_1, \ldots, X_p; Y_1, \ldots, Y_p)$ (f — многочлен)	IV	4	1
$D_i f$, $D_{X_i} f$, $\frac{\partial f}{\partial X_i}$, f'_{X_i} (f — многочлен)	IV	4	1
Df, $\frac{df}{dX}$, f' (f — многочлен одной переменной)	IV	4	1
$[D_1, D_2]$ (D_1, D_2 — дифференцирования алгебры)	IV	4	3
$\mathscr{D}(E)$ (E — алгебра)	IV	4	3
f^D (f — многочлен с коэффициентами из A, D — дифференцирование в A)	IV	4	4
$D_i f$, $\frac{\partial f}{\partial X_i}$, f'_{X_i} (f — рациональная дробь)	IV	4	4
$\frac{\partial f}{\partial x_i}$ (f — рациональная дробь, (x_i) — семейство, допускающее подстановку в f)	IV	4	4

	Глава	§	n°
$A[[X_i]]_{i\in I}$, $A[[X_{i_1}, X_{i_2}, \ldots, X_{i_p}]]$	IV	5	1
$\omega(u)$, $\omega_J(u)$ (u — формальный ряд)	IV	5	2
$\sum_{\lambda\in L} u_\lambda$, $u_{k_1}+u_{k_2}+\ldots+u_{k_n}+\ldots$ ($(u_\lambda)_{\lambda\in L}$ — суммируемое семейство формальных рядов)	IV	5	4
$f(u_1, u_2, \ldots, u_p)$ (f — формальный ряд, u_i — формальные ряды без свободного члена)	IV	5	5
$K((X_1, X_2, \ldots, X_p))$, $K((X))$	IV	5	7
$\omega(u)$ (u — формальный ряд из $K((X))$)	IV	5	7
$D_i u$, $\frac{\partial u}{\partial X_i}$ (u — формальный ряд)	IV	5	8
du, $du(X_1, \ldots, X_p; Y_1, \ldots, Y_p)$ (u — формальный ряд)	IV	5	8
A^p (A — часть поля, характеристическая экспонента которого p)	V	1	2
$\dim \mathrm{al}_K E$, $\dim_K E$ (E — расширение поля K)	V	5	3
Ω_K (K — подполе Ω)	V	7	1
$x^{p^{-e}}$, x^{1/p^e}	V	8	1
$K^{p^{-e}}$, $K^{1/p}$, $K^{p^{-\infty}}$ (K — поле, характеристическая экспонента которого p)	V	8	1
$[E:K]_S$, $[E:K]_i$	V	8	4
$\mathrm{N}_{E/K}(x)$, $\mathrm{N}_E(x)$, $\mathrm{N}(x)$	V	10	6
$\mathrm{Tr}_{E/K}(x)$, $\mathrm{Tr}_E(x)$, $\mathrm{Tr}(x)$	V	10	6
$\varphi(n)$	V	11	1
$R_n(K)$	V	11	2
Φ_n	V	11	2
F_q	V	11	3
$x \mid y$, $x \nmid y$	VI	1	5
(x)	VI	1	5
$x \equiv x' \pmod{y}$	VI	1	5
$\sup_F x_\iota$ (F — часть упорядоченяого множества E)	VI	1	8
н. о. д (x_i), н. о. к (x_i)	VI	1	8
x^+, x^-, $\lvert x\rvert$ (x — элемент решеточно-упорядоченной группы)	VI	1	11
$\sqrt{a}$ ($a \geqslant 0$ — элемент упорядоченного поля)	VI	2	4
$\lvert z\rvert$ (z — элемент $K(i)$, где K — упорядоченное поле и $i^2=-1$	VI	2	6

УКАЗАТЕЛЬ ТЕРМИНОВ

	Глава	§	n°
Абелево замыкание поля	V,	10,	3
— *расширение*	V,	10,	3
— *уравнение*	V,	10,	3
Абсолютное значение $Z \in K$ (i) (K — упорядоченное поле)	VI,	2,	6
— — в решеточно-упорядоченной группе	VI,	1,	11
Алгебра градуированная	IV,	1,	3
— *многочленов*	IV,	1,	1
— *формальных степенных рядов*	IV,	5,	1
Алгебраически зависимые элементы	V,	5,	1
— *замкнутое поле*	V,	4,	1
— — — в расширении	V,	3,	3
— *независимые элементы*	V,	5,	1
— *разделенные расширения*	V,	5,	4
— *свободная система*	V,	5,	1
— — *часть*	V,	5,	1
— *свободное семейство*	V,	5,	1
— *связанная система*	V,	5,	1
— — *часть*	V,	5,	1
— *связанное семейство*	V,	5,	1
Алгебраический элемент над полем	V,	3,	1
Алгебраическое замыкание поля	V,	4,	2
— — *поля* в расширении	V,	3,	3
— *расширение поля*	V,	3,	2
Артина теорема	V,	7,	1
Артина — Шрейера теорема	VI,	2,	3
Ассоциированные элементы	VI,	1,	5
Базис линейный расширения	V,	5,	1
— *сепарабельный трансцендентности расширения*	V,	9,	3
— *трансцендентности расширения*	V,	5,	2
Биквадратичная форма	IV,	1,	3
Бинарная форма	IV,	1,	3
Вес однородного элемента градуированной алгебры	IV,	1,	3
Взаимно простые многочлены	IV,	1,	5
— — *элементы*	VI,	1,	12
Внутреннее дифференцирование	IV,	4,	3
Градуированная алгебра	IV,	1,	3
Градуированный модуль	IV,	1,	3
Градуировка алгебры	IV,	1,	3
— *модуля*	IV,	1,	3
Галуа группа многочлена	V,	10,	3
— — *расширения*	V,	10,	1
— *расширение*	V,	10,	1
— *уравнение*	V,	10,	3

	Глава	§	n°
Группа Галуа многочлена	V,	10,	3
— — расширения	V,	10,	1
— *предупорядоченная*	VI,	1,	2
— *упорядоченная*	VI,	1,	1
Гильберта теорема	V,	11,	5
Двойной корень многочлена	IV,	2,	4
Двучленное уравнение	V,	11,	6
Дедекинда теорема	V,	7,	5
Деление евклидово многочленов	IV,	1,	5
Деления круга многочлена	V,	11,	2
— — *уравнение*	V,	11,	2
Делимости отношение	VI,	1,	5
Делители единицы	VI,	1,	5
Делитель строгий элемента	VI,	1,	5
— *элемента*	VI,	1,	5
Дискретная структура порядка	VI,	1,	3
Дискриминант базиса расширения	V,	10,	6
Дифференциал многочлена	IV,	4,	1 и 6
— полный элемента алгебры	IV,	4,	5
— рациональной дроби	IV,	4,	6
Дифференциальная форма над алгеброй	IV,	4,	5
Дифференцирование алгебры	IV,	4,	3
— *внутреннее*	IV,	4,	3
— *кольца*	IV,	4,	3
— *подалгебры* E *в* алгебре F	IV,	4,	4
— *частное* в A $[x_1, x_2, \ldots, x_n]$	IV,	4,	3
— — в $K(x_1, x_2, \ldots, x_n)$	IV,	4,	4
— — в A $[[x_1, x_2, \ldots, x_n]]$	IV,	5,	8
Допускающее подстановку семейство	IV,	3,	2
Дробный главный идеал	VI,	1,	5
Дробь несократимая	VI,	1,	11
— *рациональная*	IV,	3,	1
— — *однородная*	IV,	3,	упр. 3
— — *симметрическая*	V,	I,	1
Евклида лемма	VI,	1,	12
Евклидово деление многочленов	IV,	1,	5
— *частное*	IV,	1,	5
Единицы в кольце	VI,	1,	5
Замыкание абелево поля	V,	10,	3
Замыкание алгебраическое поля	V,	4,	2
— — — в расширении	V,	3,	3
Идеал алгебраических соотношений между x_ι	IV,	2,	1
Идеал алгебраических соотношений, которым удовлетворяет x	IV,	2,	1
— *главный дробный*	VI,	1,	5
Инвариантность порядка при трансляции	VI,	1,	1
Квадратичная форма	IV,	1,	3
Кватернарная форма	IV,	1,	3
Кольцо упорядоченное	VI,	2,	1
Конечного типа расширение	V,	2,	2
Константы в A $[X_\iota]_{\iota \in I}$	IV,	1,	3
Корень двойной многочлена	IV,	2,	4
— *из единицы*	V,	11,	1
— *квадратный* в упорядоченном поле	VI,	2,	4
— *кратный* многочлена	IV,	2,	4
— многочлена	IV,	2,	4
— n-й степени из единицы	V,	11,	1,
— *первообразный* n-й степени из единицы	V,	11,	1

	Глава	§	n°
Корень простой многочлена	IV,	2,	4
— *тройной* многочлена	IV,	2,	4
— *четырехкратный* многочлена	IV,	2,	4
Коэффициент старший ненулевого многочлена из $A[X]$	IV,	1,	3
Коэффициенты многочлена	IV,	1,	1
— формального ряда	IV,	5,	1
Кратное единицы	VI,	1,	5
— строгое элемента	VI,	1,	5
— элемента	VI,	1,	5
Кратность корня многочлена	IV,	2,	4
Кратный корень многочлена	IV,	2,	4
Критерий Маклейна	V,	8,	2
Кубическая форма	IV,	1,	5
К-автоморфизм расширения поля К	V,	2,	1
К-дифференцирование расширения поля К	V,	9,	1
К-изоморфизм расширения поля К	V,	2,	1
К-изоморфные расширения	V,	2,	1
К-эндоморфизм расширения поля К	V,	2,	1
Лагранжа интерполяционная формула	IV,	2,	4
Лейбница формула	IV,	4,	3
Лексикографическое произведение	VI,	1,	6
Лемма Евклида	VI,	1,	12
Линейная форма	IV,	1,	3
Линейно разделенные расширения	V,	2,	3
— *свободное семейство*	V,	5,	1
Линейный базис расширения	V,	5,	1
Маклейна критерий	V,	8,	2
Максимальное упорядоченное поле	VI,	2,	5
Минимальный многочлен алгебраического элемента	V,	3,	1
Многочлен	IV,	1,	1
— *деления круга*	V,	11,	2
— *минимальный* алгебраического элемента	V,	3,	1
—, меняющий знак в интервале	VI,	2,	4
—, не содержащий свободного члена	IV,	1,	1
— — — X_ι, $\iota \in J$	IV,	1,	2
— *однородный* полной степени p	IV,	1,	3
— — степени p относительно X_ι, $\iota \in J$	IV,	1,	3
— от n переменных	IV,	1,	2
— *сепарабельный*	V,	7,	6
— степени $\geqslant p$ $(> p)$	IV,	1,	3
— *унитарный*	IV,	1,	3
Многочлены взаимно простые	IV,	1,	5
Множитель несепарабельный степени алгебраического расширения	V,	8,	4
— *сепарабельный* степени алгебраического расширения	V,	8,	4
Модуль градуированный	IV,	1,	3
Моноид предупорядоченный	VI,	1,	2
— *упорядоченный*	VI,	1,	1
Наибольший общий делитель двух многочленов в $K[X]$	IV,	1,	5
— — — (н. о. д.) элементов	VI,	1,	8
Наименьшее общее кратное двух многочленов в $K[X]$	IV,	1,	5

	Глава	§	n°
Наименьшее общее кратное (н. о. к.) элементов	VI,	1,	8
Независимые элементы	VI,	1,	12
Неприводимый многочлен	IV,	1,	5
Неравенство треугольника в K (i) (K упорядочено)	VI,	2,	6
Несократимая дробь	VI,	1,	11
Норма элемента сепарабельного алгебраического расширения	V,	10,	6
Нормальное расширение	V,	6,	3
— *уравнение*	V,	6,	3
Нормальный базис	V,	10,	8
Нуль многочлена	IV,	2,	4
Ньютона формула	V,	1,	3
n-арная форма	IV,	1,	3
Образующих система надполя	V,	2,	2
Однородная составляющая степени p многочлена	IV,	1,	3
— — — p формального ряда	IV,	5,	2
Однородная составляющая элемента в градуированной алгебре	IV,	1,	3
— — — в градуированном модуле	IV,	1,	3
Однородный многочлен	IV,	1,	3
— *элемент* в градуированной алгебре	IV,	1,	3
— — в градуированном модуле	IV,	1,	3
Одночлен	IV,	1,	1
Остаток при евклидовом делении двух многочленов	IV,	1,	5
Отношение делимости	VI,	1,	5
— — *тривиальное*	VI,	1,	5
Отрицательная часть элемента	VI,	1,	11
Отрицательный элемент	VI,	1,	3
Первообразный корень n-й степени из единицы	V,	11,	1
Переменная	IV,	1,	1
Подрасширение	V,	2	
Подстановка формальных рядов в формальный ряд	IV,	5,	5
— x_ι место X_ι в многочлен	IV,	2,	1
Поле алгебраически замкнутое	V,	4,	1
— — — в расширении	V,	3,	3
— *корней* многочлена	V,	4,	2
— — *n-й* степени из единицы	V,	11,	2
— *промежуточное*	V,	2	
— *простое*	V,	1,	1
— *рациональных дробей*	IV,	3,	1
— *совершенное*	V,	7,	3
— *упорядоченное*	IV,	2,	2
— — *максимальное*	VI,	2,	2
— *формальных рядов*	IV,	5,	7
Положительный элемент	VI,	1,	3
Положительная часть элемента	VI,	1,	11
Порядок обобщенного формального ряда	IV,	5,	7
— *полный формального ряда*	IV,	5,	2
— *формального ряда* относительно X_ι, $\iota \in J$	IV,	5,	2
Правило знаков	VI,	2,	1 и 2
Предупорядоченная группа	VI,	1,	2
Предупорядоченный моноид	VI,	1,	2
Применение дифференцирования к коэффициентам многочлена	IV,	5,	4
— *представления* к коэффициентам многочлена	IV,	1,	2
Примитивный элемент	V,	7,	7
Принцип продолжения алгебраических тождеств	IV,	2,	5

	Глава	§	n°
Присоединение (поле, полученное присоединением)	V	2	2
Произведение лексикографическое упорядоченных групп	VI	1	6
Производная многочлена в $A[X]$	IV	4	1
— *частная* многочлена	IV	4	1
— — рациональной дроби	IV	4	4
Промежуточное поле	V	2	
Простое поле	V	1	1
— *расширение*	V	2	2
Простой корень	IV	2	4
P-базис	V	8, упр.	1
Радикальное расширение	V	8	4
Радикальный элемент	V	8	1
Разложение в формальный ряд рациональной дроби	IV	5	4 и 5
Разложения теоремы	VI	1	10
Размерность алгебраическая расширения	V	5	2 и упр. 1
Расширение абелево	V	10	3
— *алгебраическое*	V	3	2
— *Галуа*	V	10	1
— *конечного типа*	V	2	2
— *нормальное*	V	6	3
— *поля*	V	2	
— *простое*	V	2	2
— *радикальное*	V	8	4
— *сепарабельное*	V	7	2
— *трансцендентное*	V	3	2
— *универсальное*	V	6	1
— *упорядоченное поля*	VI	2	3
— *циклическое*	V	11	5
— *чисто трансцендентное*	V	5	1
— *чистое*	V	5	1
Расширения, алгебраически разделенные	V	5	4
Расширения Галуа (основная теорема)	V	10	5
— *линейно разделенные*	V	2	3
— *сопряженные*	V	6	2
Рациональная дробь	IV	3	1
— *функция*	IV	3	4
Ряд обобщенный формальный	IV	5	7
— *формальный*	IV	5	1
Свободный член многочлена	IV	1	1
— — формального ряда	IV	5	2
Семейство, алгебраически свободное	V	5	1
—, — связанное	V	5	1
—, допускающее подстановку в рациональную дробь	IV	3	2
Семейство линейно свободное	V	5	1
— суммируемое формальных рядов	IV	5	4
Сепарабельное расширение	V	7	2
Сепарабельный алгебраический элемент	V	7	6
— *базис трансцендентности*	V	9	3
— *многочлен*	V	7	6
Симметрические функции	I	1	
— *рациональные дроби*	I	1	
Система, алгебраически свободная	V	5	1
—, — связанная	V	5	1
След элемента сепарабельного алгебраического расширения	V	10	6
Сложение неравенств	IV	1	1
Совершенное поле	V	7	3
Сопряженные подрасширения	V	6	2
— *элементы*	V	6	2

	Глава	§	n°
Составляющая однородная элемента градуированной алгебры	IV,	1,	3
Старший коэффициент многочлена	IV,	1,	3
Степень многочлена относительно X, $\subset J$	IV,	1,	3
— *полная многочлена*	IV,	1,	3
— — *рациональной дроби*	IV,	3,	1
— *рациональной дроби* относительно некоторой переменной	IV,	3,	1
— *расширения*	V,	2,	1
— *трансцендентности расширения*	V, 5,	2	и упр. 1
— *элемента градуированной алгебры*	IV,	1,	3
— — *градуированного модуля*	IV,	1,	3
Строго отрицательный элемент	VI,	1,	3
— *положительный элемент*	VI,	1,	3
Структура дискретного порядка	VI,	1,	3
— *порядка*, согласованная со структурой группы	VI,	1,	1
— — согласованная со структурой кольца	VI,	2,	1
— — согласованная со структурой моноида	VI,	1,	1
— *предпорядка*, согласованная со структурой коммутативного моноида	VI,	1,	2
Сумма прямая упорядоченных групп	VI,	1,	6
Суммируемое семейство формальных рядов	IV,	5,	4
Тейлора формула	IV,	5,	8
Теорема Артина	V,	7,	1
Теорема Артина — Шрейера	VI,	2,	3
— *Гильберта*	V,	11,	5
— *Дедекинда*	V,	7,	5
— *основная о расширениях Галуа*	V,	10,	5
— *разложения*	VI,	1,	10
— *Штейница*	V,	4,	2 и V, 5,2
— *Эйлера — Лагранжа*	VI,	2,	6
Тернарная форма	IV,	1,	3
Трансцендентное расширение	V,	3,	2
Трансцендентный элемент	V,	3,	1
Тривиальное отношение делимости	VI,	1,	5
Тройной корень многочлена	IV,	2,	4
Универсальное расширение	V,	6,	1
Унитарный многочлен	IV,	1,	3
Упорядоченная группа	VI,	1,	1
Упорядоченное кольцо	VI,	2,	1
— *поле*	VI,	2,	2
— *расширение*	VI,	2,	3
Упорядоченный моноид	VI,	1,	1
Уравнение абелево	V,	10,	3
— *Галуа*	V,	10,	3
— *деления круга*	V,	11,	2
— *двучленное*	V,	11,	6
— *нормальное*	V,	6,	3
Форма бинарная	IV,	1,	3
— *биквадратичная*	IV,	1,	3
— *внешняя дифференциальная* над алгеброй	IV,	4,	упр. 14
— *дифференциальная* над алгеброй	IV,	4,	5
— *квадратичная*	IV,	1,	3
— *кватернарная*	IV,	1,	3
— *кубическая*	IV,	1,	3

	Глава	§	n°
Форма *линейная*	IV,	1,	3
— *степени p*	IV,	1,	3
— *тернарная*	IV,	1,	3
— *n-арная*	IV,	1,	3
Формула интерполяционная Лагранжа	IV,	2,	4
— *Лейбница*	IV,	4,	3
— *Ньютона*	V,	I,	3
— *Тейлора*	IV,	5,	8
Функция полиномиальная	IV,	2,	3
— *рациональная*	IV,	3,	4
Функция симметрическая		I,	1
— *Эйлера*	V,	11,	1
— *элементарная симметрическая*	V ,	I,	1
Характеристическая экспонента	V,	1,	2
Целый в поле	VI,	1,	5
Частная производная многочлена	IV,	4,	1
— — рациональной дроби	IV,	4,	4
Частное дифференцирование алгебры многочленов	IV,	4,	3
— — — формальных рядов	IV,	5,	8
— — поля рациональных дробей	IV,	4,	4
— евклидово многочлена при его делении на унитарный многочлен	IV,	1,	5
Часть, алгебраически свободная	V,	5,	1
—, — связанная	V,	5,	1
— *отрицательная элемента*	VI,	1,	11
— *положительная элемента*	VI,	1,	11
Четырехкратный корень многочлена	IV,	2,	4
Чисто трансцендентное расширение	V,	5,	1
Чистое расширение	V,	5,	1
Чистый базис	V,	5,	1
Член многочлена	IV,	1,	1
— *полной степени p* в многочлене	IV,	1,	3
— — — в формальном ряде	IV,	5,	2
— *свободный* многочлена	IV,	1,	1
— — формального ряда	IV,	5,	2
— *степени p* относительно X_ι, $\iota \in J$, в многочлене	IV,	1,	3
— — — — — в формальном ряде	IV,	5,	2
Член формального ряда	IV,	5,	1
Штейница теорема	V, 4, 2 и V, 5, 2		
Эйлера — Лагранжа теорема	VI,	2,	6
Эйлера функция	V,	11,	1
Экспоненты характеристическая	V,	1,	2
Экстремальный элемент	VI,	1,	13
Элемент алгебраический расширения	V,	3,	1
— *из A кратности* $\geqslant h$ относительно многочлена из $A[X]$	IV,	2,	4
— *отрицательный*	VI,	1,	3
— *положительный*	VI,	1,	3
— *примитивный расширения*	V,	7,	7
— *радикальный расширения*	V	8,	1
— *сепарабельный алгебраический расширения*	V,	7,	6
— *строго отрицательный*	VI,	1,	3

	Глава	§	n°
Элемент строго положительный	VI,	1,	3
— *трансцендентный расширения*	V,	3,	1
— *экстремальный* . .	VI,	1,	13
Элементарные симметрические функции	V,	I,	1
Элементы алгебраически зависимые расширения	V,	5,	1
— — *независимые* расширения	V,	5,	1
Элементы ассоциированные	VI,	1,	5
— *взаимно простые* . .	VI,	1,	12
Элементы независимые	VI,	1,	12
— — *в совокупности* . .	VI,	1,	12
— — *попарно*	VI,	1,	12
— *однородные градуированного модуля*	IV,	1,	3
— — *градуированной алгебры*	IV,	1,	3
— *сопряженные расширения*	V,	6,	2